# Secunia Corporate Software Inspector (CSI)

## Complete – Flexible – Unique

## The Secunia CSI 7.0 works the way you do

**Secunia CSI 7.0 – Technical User Guide**

**Rev. 03-Sep-2013**

# Contents


**Secunia Corporate Software Inspector (CSI) ..... 1**
**Contents ..... 2**
**The Secunia CSI 7.0 ..... 5**
The Scan Process – How Does it Work? ..... 5
Targeted Patch Management ..... 6
The Secunia CSI 7.0 Vulnerability Management Life Cycle ..... 6
System Requirements ..... 7
The Secunia CSI 7.0 with Scanning and Patching Capabilities ..... 7
What's New ..... 8
Superseded Secunia CSI 6 Features ..... 9
**Getting Started ..... 10**
Download and Install the Secunia CSI IE Plugin ..... 10
Download and Install the Secunia Daemon ..... 10
Tips ..... 12
**Dashboard ..... 13**
**Scanning ..... 14**
Scan Types ..... 14
Agent-based Scan – Requirements (Windows) ..... 15
Agent-based Scan – Requirements (Mac OS X) ..... 15
Remote/Agent-less Scan – Requirements (Windows) ..... 15
Remote Scanning Via CSI (Agent-less Scan) ..... 16
Quick Scan ..... 17
Scan Groups ..... 17
Scan Progress ..... 17
System Center Configuration Manager Inventory Import ..... 18
System Center Configuration Manager Import Schedules ..... 19
Remote Scanning Via Agents ..... 20
Network Appliance Agents ..... 21
Network Appliance Groups ..... 21
Download Network Agent ..... 21
Scanning Via Local Agents ..... 22
Single Host Agents ..... 23
Download Local Agent ..... 23
PSI for Windows and Android ..... 25
PSI for Windows ..... 25
PSI for Android ..... 27
Scanning Mac OS X ..... 28
Download the CSIA for Apple Mac OS X ..... 28
Prepare Your MAC ..... 28
Install MAC Agent ..... 29
Scanning Red Hat Enterprise Linux (RHEL) ..... 30
Installing the CSIA for Red Hat Linux ..... 30
Filter Scan Results ..... 31
Scan Paths ..... 31
Custom Scan Rules ..... 32
Completed Scans ..... 32
**Results ..... 33**
Sites ..... 33
Smart Groups ..... 33
Host Smart Groups ..... 35
Overview and Configuration ..... 35
Configured Host Groups ..... 35

Product Smart Groups ..... 36
Overview and Configuration ..... 36
Configured Product Groups ..... 36
Advisory Smart Groups ..... 37
Overview and Configuration ..... 37
Zero-Day Advisories (Optional Module) ..... 37
Configured Advisory Groups ..... 37
**Reporting ..... 38**
Report Configuration ..... 38
Smart Group Notifications ..... 39
Database Access ..... 40
Database Console ..... 40
Database Cleanup ..... 40
Scheduled Exports ..... 41
**Patching ..... 42**
Secunia Package System (SPS) ..... 42
SPS Concepts and Terminology ..... 43
What does a SPS package consists of? ..... 43
Applicability Rules ..... 43
SPS Package ..... 43
Execution Flow Script ..... 43
Files ..... 43
Creating a Patch with the Secunia Package System (SPS) ..... 44
Create an Update Package ..... 45
Create an Uninstall Package ..... 45
Create a Custom Package ..... 46
The SPS Package Creation Wizard ..... 46
Step 1 of 4: Package Configuration ..... 46
Step 2 of 4: Package Contents ..... 47
Step 3 of 4: Applicability Criteria - Paths ..... 48
Step 4 of 4: Applicability Criteria - Rules ..... 49
Agent Deployment ..... 50
Add Proxy Settings ..... 50
WSUS/System Center Configuration Manager ..... 51
Available ..... 51
Deployment ..... 51
Deploying the Update Package Using WSUS ..... 52
Deploying the Update Package Using System Center Configuration Manager ..... 52
Configuration ..... 52
WSUS/System Center Configuration Manager ..... 52
Step 1 – Connection Status ..... 53
Step 2 – Certificate Status ..... 54
Step 3 – Group Policy Status ..... 55
Setting Up Clients to Access WSUS ..... 56
Third-Party Integration ..... 57
Create and Publish the Package ..... 57
**Administration ..... 58**
Overview ..... 58
User Management ..... 59
Create a New Administrator ..... 59
Create a New User ..... 59
Active Directory (Requires the Secunia CSI Plugin) ..... 60
IP Access Management (Requires the Secunia CSI Plugin) ..... 61
Password Policy Configuration ..... 62
**Configuration ..... 63**

Suggest Software ..... 63
Settings ..... 63
Scan Settings ..... 63
Instant Access ..... 63
Collect Network Info ..... 63
Zombie File Settings ..... 63
Default Recipient Settings ..... 63
Windows Update Settings ..... 64
Debug Logging ..... 64
Log Messages ..... 64
Activity Log ..... 65
VIM Integration ..... 65
Accounts Overview ..... 65
Asset Lists ..... 65
Security ..... 66
Change Password ..... 66
Password Recovery Settings ..... 66
**Further Information ..... 67**
**About Secunia ..... 67**
**Disclaimer ..... 68**

# The Secunia CSI 7.0

The Secunia CSI 7.0 is a Vulnerability and Patch Management Software Solution that completes and targets the Patch Management process. It combines Vulnerability Intelligence, Vulnerability Scanning, and Patch Creation with Patch Deployment Tool Integration to enable targeted, reliable, and cost-efficient Patch Management.

Vulnerability and Patch Management are critical components of any security infrastructure because it enables proactive detection and remediation of vulnerabilities before they are actively exploited and your security compromised. With the Secunia CSI, IT Operations and Security Teams are empowered to take control of the Vulnerability Threat from both Microsoft and non-Microsoft (third-party) product vulnerabilities, covering Microsoft Windows, Mac OSX, Android and Red Hat Enterprise Linux.

The Secunia scanning technology takes a different approach than other vulnerability scanning solutions by conducting non-intrusive scans to accurately identify all installed products and plugins on the system.

The Secunia CSI integrates seamlessly with Microsoft WSUS, SC2012 and System Center Configuration Manager (SCCM) 2007.

## The Scan Process – How Does it Work?

The first step in scanning a system is to collect specific metadata from primarily .EXE, .DLL, and .OCX files on the system being scanned. Metadata is generic non-sensitive text strings embedded in the binary files from the vendors of the products. This data is collected and then sent to Secunia's Secure Data Processing Cloud where it is processed and parsed.

Detailed information about which data is collected can be found in the Secunia Data Security Factsheet available for download in the following location:

http://secunia.com/?action=fetch&filename=Secunia_DataSecurity.pdf

The data is then matched against Secunia File Signatures, which are rules that match the raw metadata to an actual product installation.

Part of this matching process also results in an exact version being extracted from the metadata. This means that after the initial parsing the Secunia CSI knows exactly which products are on the system and their exact version – a precise inventory of software on the system.

The inventory of software is then compared against the unique Secunia Advisory and Vulnerability Database, which contains the most accurate and current Vulnerability Intelligence available.

The result is a precise inventory of products, their versions, the security state of each, along with a direct reference to any corresponding Secunia Advisory detailing the exact vulnerabilities and their Secunia assessed criticality and impact.

Since the scan process works by looking at the actual files on the system being scanned, the result is extremely reliable as a product cannot be installed on a system without the actual files required being present.

This in turn means that the Secunia CSI rarely identifies false-positives and you can use the results from the Secunia CSI immediately without doing additional data mining.

The Secunia CSI is flexible and scalable when it comes to scanning a corporate network and you can choose to use Agent, Agent-less, or a combination of both scanning methods in the same environment.

Refer to Scanning for further information about the different scanning approaches.

# Targeted Patch Management

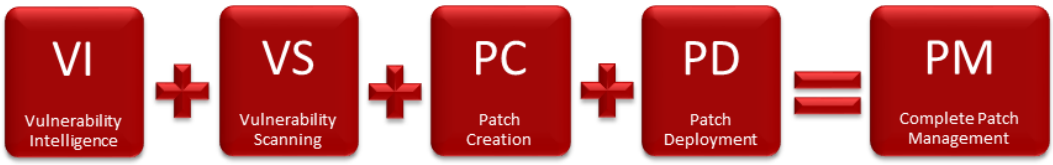
Patching of vulnerable software, in particular third-party software which is not supported by Microsoft WSUS, has been a cumbersome and resource intensive process causing many enterprises to either neglect patching or only patch very few non-Microsoft applications.

Through the seamless Microsoft WSUS and System Center Configuration Manager integration with the Secunia CSI, the patching process has been simplified and can be conducted with a few simple clicks.

When establishing best practice recommendations for targeted patch management processes - as well as any Patch Management solution that supports this - four elements are essential:

- Vulnerability Intelligence (VI)
- Vulnerability Scanning (VS)
- Patch Creation (PC)
- Patch Deployment (PD)

Targeted Patch Management (PM) is basically the sum of these four elements:

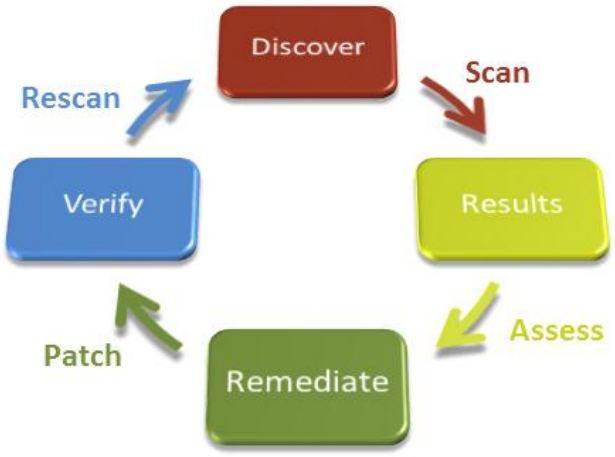



# The Secunia CSI 7.0 Vulnerability Management Life Cycle

Vulnerability management is a critical component of any security infrastructure because it enables proactive detection and remediation of security vulnerabilities.

A process to identify vulnerable products, including products not authorized in an organization's environment, paired with effective patch management is an absolute must to reduce the window of exposure and eliminate the root cause of a potential compromise.

The Secunia CSI automates all steps of the vulnerability management lifecycle, allowing organizations to strengthen the security of their networks.



# System Requirements

To use the Secunia CSI 7.0 console your system should meet the following requirements:

- Min resolution: 1024x768
- The latest version of Internet Explorer (Scan results can also be viewed from other browsers)
- Internet connection capable of connecting to https://csi7.secunia.com
- The addresses crl.verisign.net, crl.thawte.com and https://*.secunia.com/ should be white-listed in the Firewall/Proxy configuration
- First-Party cookie settings at least to Prompt (in Internet Explorer)
- Allow session cookies
- A PDF reader

# The Secunia CSI 7.0 with Scanning and Patching Capabilities

To successfully scan and create updates the following should also be present when using the Secunia CSI:

- Internet Explorer 8 or higher with the CSI Plugin installed
- WSUS installer (Administration console only)
- Visual C runtime
- Microsoft .NET Framework runtime 4 or later
- If the WSUS Self-Signed Certificate is going to be used, and the user wishes to provision the certificate through the **Patching > WSUS/SCCM > Deployment** function, Remote Registry service must be enabled on the clients
- Select the target hosts where the certificate is to be installed (CTRL+ mouse click for multiple selection), right-click and select **Verify and Install Certificate**

# What's New

- **Administration –** Create and administer Secunia CSI accounts using role based account management, where each CSI user is created and assigned a set of roles and limitations as appropriate. These roles determine which parts of the Secunia CSI the user has access to and limits what the user can view and scan.
- **Browser Interface (SaaS) –** Login to the Secunia CSI from any browser (the latest version of IE recommended) without installing a local console and synchronizing data to a local database.
- **Instant Access –** Updates your scan results as new Vulnerability Intelligence pertaining to your existing scan results emerges.
- **Package Configuration and Integration –** Configure your patching package using dynamic check box options, based on product functionality, using the Secunia Package System (SPS). You can also target specific languages and approve packages before they are published. The package configuration, based on the product family, is retained for future use.
- **Password Policy Configuration –** Configure the password policy for all users.
- **Enhanced and Fully Integrated Smart Groups –** Smart Group types now include **Host**, **Product** and **Advisory** Smart Groups. **All Hosts**, **All Products** and **All Advisories** are the default Smart Groups for each category and cannot be edited or deleted. You can create and manage additional Smart Groups to match your specific requirements.
- **PSI for Windows and Android –** Integrate with the Secunia PSI for scanning Windows and Android devices connected to your network.
- **Zero-Day Vulnerability Support (Optional Module) –** Receive an overview of all zero-day advisories relevant to products on your system. A zero-day vulnerability is a vulnerability that has only been discovered by hackers and is being actively exploited. Consequently, users are at risk of being attacked by hackers, using the vulnerability to gain access to the computers, programs, data and systems, running the vulnerable system.

# Superseded Secunia CSI 6 Features

- **Ignore Rules –** This feature was previously used to filter out (after a scan) specific content from results and reports. The Secunia CSI 7 allows the user to create Host, Product and Advisory Smart Groups that act as custom filters to display only the content you want to see.
- **Local Database Console –** This feature was previously used to create custom SQL queries for the local database in the Secunia CSI and has been replaced with the **Reporting > Database Access >** Database Console. Furthermore, the Secunia CSI no longer runs on a Local Database on the client machine.
- **Maintenance menu –** Previously contained the Permanent Logout and Database Cleanup options and has been removed. A Logout button has been added to the top toolbar and the Database Cleanup option is now located under the **Reporting > Database Access >** Database Cleanup menu.
- **Results > Hosts –** Previously displayed all the hosts maintained within a user account and has been replaced with Host Smart Groups, where the user can view the existing configured Host Smart Groups and configure new Smart Groups.
- **Results > Programs and Operating Systems –** Previously displayed a list of all the Programs or Operating Systems found via the CSI scans and has been replaced with Product Smart Groups, where the user can view the existing configured Product Smart Groups and configure new Smart Groups.
- **Results > Secunia Advisories –** Previously displayed all advisories relevant to Insecure or End-of-Life products in the user's environment and has been replaced with Advisory Smart Groups.
- **Static Dashboard –** Previously, for each dashboard profile created, a static URL was automatically created so that the user could use the static URL to view the dashboard on any web browser. The Secunia CSI 7 now uses a browser interface which makes this feature redundant.
- **Trend Reporting –** Previously displayed as part of the **Results > Hosts** and **Results > Sites** pages and has been removed as all results are now viewed through Smart Groups.
- **User Management –** Previously, this feature was used by the Secunia CSI main account to create other Secunia CSI accounts. Accounts, Shadow Accounts and Reporting on Sub-accounts and has been replaced with a new Administration infrastructure.

# Getting Started

The Secunia CSI 7.0 solution is accessible via https://csi7.secunia.com.

You will be prompted for authentication with your username/password. Please use the credentials supplied by Secunia personnel. The initial password issued by Secunia is a one-time only password that must be changed upon the first login. The new password must contain a minimum of eight characters, or comply with the criteria defined in your custom Password Policy Configuration.

## Download and Install the Secunia CSI IE Plugin

The first time you login to the Secunia CSI, click the link on the bottom of the page and follow the on-screen instructions to download and install the CSI Plugin to enable scanning and patching. Please note that the plugin is only compatible with Internet Explorer version 8 or higher.

The CSI Plugin is installed locally and must be installed on the machine you are running the Secunia CSI console from. Once the CSI Plugin has been installed the download link is removed from the page.

## Download and Install the Secunia Daemon

The Secunia Daemon is a stand-alone executable that executes various schedules configured in the Secunia CSI console. It runs as a background service with no user interaction. You can download the Secunia Daemon from http://secunia.com/downloadcsi/.

The Secunia Daemon integrates a number of local data sources in your network with the Secunia Cloud. It should be deployed to a node in the network that has high availability (for example, the server running the SCCM or SQL server). Once deployed, the Daemon will regularly scan the following data sources, based on the configuration created in the Secunia CSI:

- Active Directory
- SCCM Import (SQL + WSUS)
- Scheduled Exports
- WSUS State Change

> ⚠ Since the Secunia Daemon is connecting directly to the Secunia servers and the System Center 2012 Configuration Manager database server unattended, you must provide the appropriate connection details during installation. The SQL Host, SQL Port and SQL Database must be set to enable it to perform unattended import from the System Center 2012 Configuration Manager database.
>
> The Secunia Daemon should only be deployed once to avoid two instances competing to retrieve the schedules.

To install the Secunia Daemon:

1. Double-click the Secunia Daemon installer icon and follow the wizard instructions.
2. Accept the End User License Agreement and click **Next**.
3. Enter the Secunia Daemon Proxy Settings (host name, port, user name and password), if required. The values in populated fields are fetched from the current user's Internet Explorer proxy settings. Click **Next**.
4. Enter the User Name and Password of your Secunia account and click **Install**.
5. Enter the credentials for a user with permissions to access the data sources read by the Daemon. The configuration parameters are set in the CSI interface, but the schedules are executed by the Daemon, and it must be authorized to read the appropriate sources. This could be done, for example, by creating a service user in the domain.
   - SCCM Inventory import: SQL database of System Center Configuration Manager.
   - WSUS: connect to the WSUS server and read state.
   - Active Directory: associated with the Domain that is being scanned. The user name must be entered in the <username>@<AD domain> format. Click **Next**.
6. Click **Finish** to close the Secunia Daemon setup.

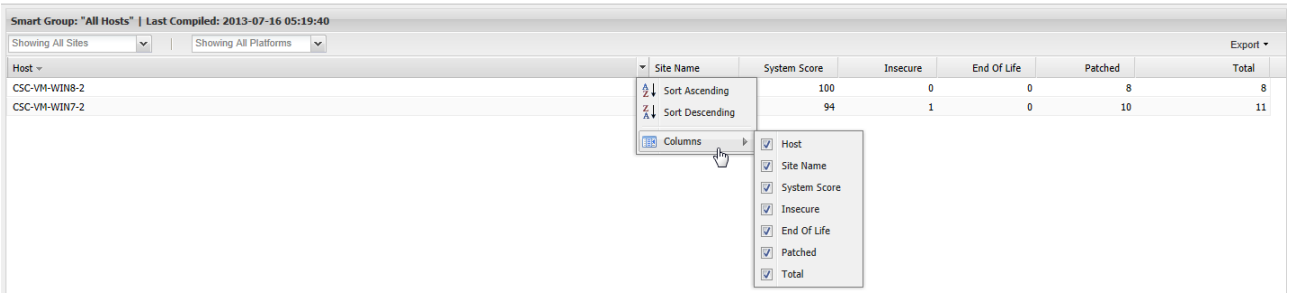
The Secunia Daemon uses the System Center 2012 Configuration Manager SQL Database Settings that are specified in the Configure dialog. If those settings haven't yet been specified when the Secunia Daemon has been run then it will check for them again in 10 minutes and every 10 minutes afterwards until it gets them.

The Secunia Daemon checks with Secunia every 10 minutes to download new schedules or fetch changes to existing schedules as long as it is not in the process of processing scans.

The results are displayed in the Secunia CSI Completed Scans page.

# Tips

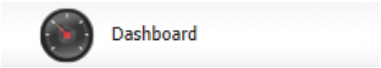
**Tip!** You can define the sorting of both lines and columns in any grid view to create the layout that best suits your needs. Click the right hand side of any of the column headings to view the available display options. The column's position can be modified by dragging and dropping the selected column to the desired position.




**Tip!** You can click **Export** in any grid view to copy the displayed information to the clipboard or save as a CSV file. You can configure the file by hiding columns in the grids prior to export.

**Tip!** You can click **Help** or press **F1** to open a help topic associated with the currently selected page in the Secunia CSI console.

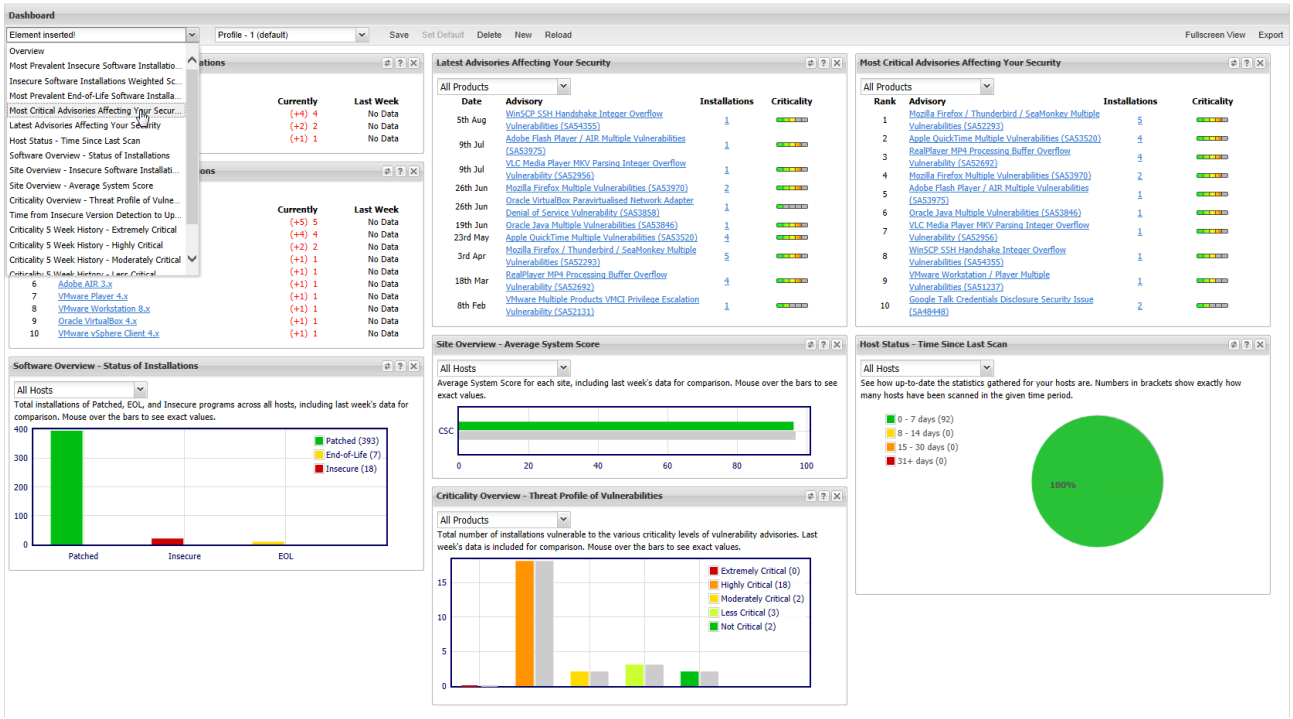
# Dashboard




The Dashboard provides an overview of your hosts with the help of various "portlets". Portlets are a collection of components that graphically display key data and allow you to create profiles which can display a unique combination of portlets.

The first time you login to the Secunia CSI console the Dashboard page will only display the Overview portlet. Select the Dashboard elements you want to view from the drop-down list on the upper left of the page. You can then either save the profile or, if you have created several profiles, set it as the default profile. You can also delete, add a new profile or reload the current profile view.

Click in any portal to refresh the data displayed. You can further filter the data in certain portlets which allow Smart Group selection.


Dashboard
Element inserted!
Profile - 1 (default)
Save
Set Default
Delete
New
Reload
Fullscreen View
Export
Overview
Most Prevalent Insecure Software Installatio...
Insecure Software Installations Weighted Sc...
Most Prevalent End-of-Life Software Installa...
Most Critical Advisories Affecting Your Secur...
Latest Advisories Affecting Your Security
Host Status - Time Since Last Scan
Software Overview - Status of Installations
Site Overview - Insecure Software Installati...
Site Overview - Average System Score
Criticality Overview - Threat Profile of Vulne...
Time from Insecure Version Detection to Up...
Criticality 5 Week History - Extremely Critical
Criticality 5 Week History - Highly Critical
Criticality 5 Week History - Moderately Critical
Currently
Last Week
Latest Advisories Affecting Your Security
All Products
Date
Advisory
Installations
Criticality
Most Critical Advisories Affecting Your Security
Rank
Advisory
Installations
Criticality
Software Overview - Status of Installations
All Hosts
Total installations of Patched, EOL, and Insecure programs across all hosts, including last week's data for comparison. Mouse over the bars to see exact values.
Patched (393)
End-of-Life (7)
Insecure (18)
Site Overview - Average System Score
All Hosts
Average System Score for each site, including last week's data for comparison. Mouse over the bars to see exact values.
CSC
Host Status - Time Since Last Scan
All Hosts
See how up-to-date the statistics gathered for your hosts are. Numbers in brackets show exactly how many hosts have been scanned in the given time period.
0 - 7 days (92)
8 - 14 days (0)
15 - 30 days (0)
31+ days (0)
100%
Criticality Overview - Threat Profile of Vulnerabilities
All Products
Total number of installations vulnerable to the various criticality levels of vulnerability advisories. Last week's data is included for comparison. Mouse over the bars to see exact values.
Extremely Critical (0)
Highly Critical (18)
Moderately Critical (2)
Less Critical (3)
Not Critical (2)

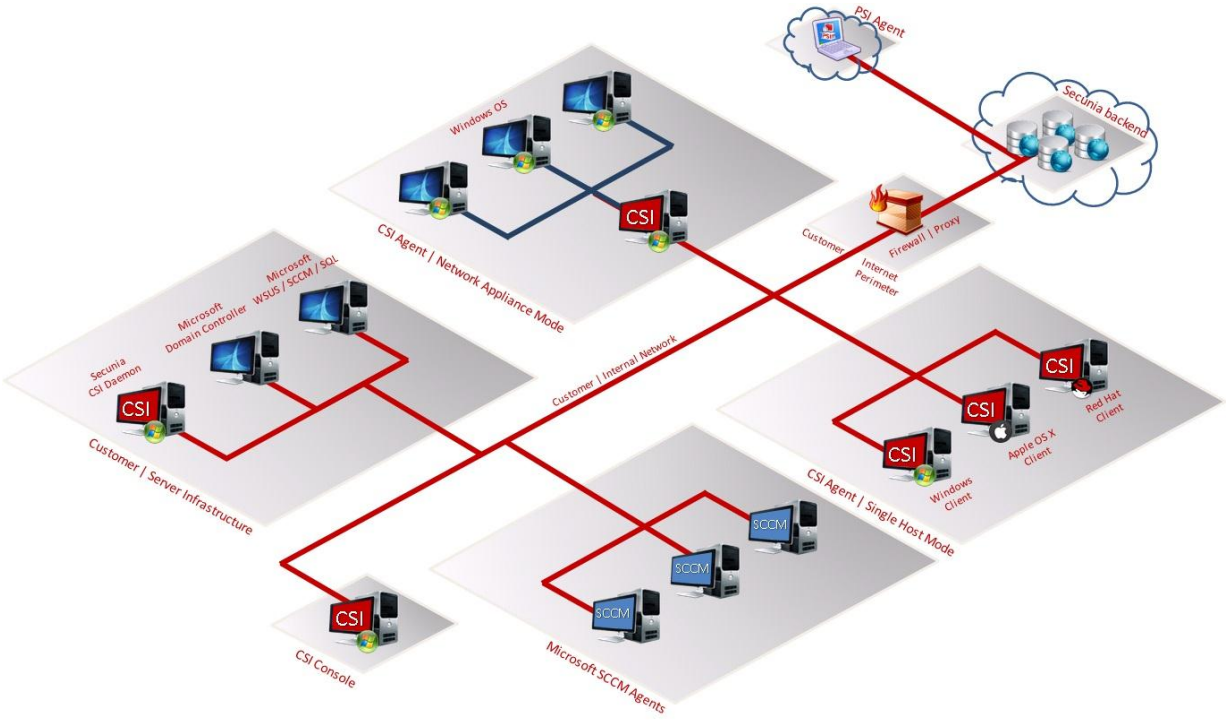
# Scanning

## Scan Types

The Secunia CSI allows scanning of target hosts using the following approaches:

- Single Host Agent-based scans are conducted by the Secunia CSI Agent that can be installed in different modes: Single Host mode, Network Appliance mode, or Command Line mode.
- Alternatively, you can scan the target hosts by launching a scan from the system where the Secunia CSI console is running. By using this approach, no software is installed in the target hosts. The scanning is performed using standard operating system services. This scan is also referred to as a "remote scan".
- You can also benefit from the integration between the Secunia CSI and the Secunia PSI. The Secunia PSI is designed to be used in environments where IT managers want to have visibility and patching control although their users have local Administrative rights to their own systems. The Secunia PSI also provides visibility and patching control of corporate devices that are not connected to the corporate domain.

The various types of scan are shown below:




Note that if the WSUS Self-Signed Certificate will be used to sign the update packages created by the Secunia CSI, you can use a different certificate as an alternative.

⚠ Administrators must ensure that the Secunia CSI, and its scanning Agent respectively, have access to all necessary system and online resources which allow the application to run as intended. The addresses crl.verisign.net, crl.thawte.com and https://*.secunia.com/ should be white-listed in the Firewall/Proxy configuration to ensure that the client system is allowed access to these online resources.

# Agent-based Scan – Requirements (Windows)

The flexibility offered by the Secunia CSI ensures that it can be easily adapted to your environment.

If you choose to scan using the installable Agent (Agent-based scans), as described in Single Host Agents, the following requirements should be present in the target hosts:

- Administrative privileges (to install the CSI Agent – csia.exe)
- Microsoft Windows XP, 2003, 2008, Vista, 7 or 8
- Internet Connection – SSL 443/TCP to https://*.secunia.com/
- Windows Update Agent 2.0 or later

# Agent-based Scan – Requirements (Mac OS X)

The following requirements should be met before installing the Single Host Agent on an Intel-based Mac OS X machine:

- Supported Systems:
  10.5 Leopard/10.6 Snow Leopard/10.6 Snow Leopard Server/10.7 Lion/10.8 Mountain Lion
- Administrator privileges at minimum ('root' privileges required for the installation)
- Internet Connection – SSL 443/TCP to https://*.secunia.com
- The user installing the agent must have 'execute' permissions on the file (chmod +x)

# Remote/Agent-less Scan – Requirements (Windows)

If you prefer to scan without installing the CSI Agent (Agent-less scans), the following requirements should be present in the target hosts:

- Ports 139/TCP and 445/TCP open inbound (on hosts)
- File sharing enabled on hosts
- Easy/simple file sharing **disabled**
- Windows Update Agent 2.0 or later

Required Windows services started on hosts:

- Workstation service
- Server service
- Remote Registry service (by default is disabled on Win7/Vista)
- COM+ services (COM+ System Application: Set to Automatic)

When performing Remote/Agent-less scans, the result may be displayed as **Partial** in the Completed Scans page. This is caused by the Windows Firewall default settings that block the RPC dynamic ports.

On the host, in Windows Firewall, the user should create an inbound rule to allow inbound traffic for all products that use RPC dynamic ports.

To create the rule:

- From Windows **Control Panel** (View by Category) **> System and Security > Windows Firewall**, select **Advanced settings**
- Select **Inbound Rules** in the **Windows Firewall with Advanced Security on Local Computer** pane and then select **New Rule** in the **Actions** pane
- The New Inbound Rule wizard opens
- Select **Custom rule** and click **Next**
- Select **All programs** and click **Next**
- In the Protocol and Ports window:
  - From the **Protocol type:** drop-down list, select **TCP**
  - From the **Local port:** drop-down list, select **RPC Dynamic Ports**
- Click **Next** until the Profile window appears:
  - Deselect **Private** and **Public**, select **Domain** and click **Next**
  - Give the rule a name, for example: **Secunia CSI**
  - Click **Finish**

Once you have created the rule, use the Secunia CSI console to perform a remote scan of the PC. The host will connect to Windows Update and the scan status should be displayed as **Success** in the Completed Scans page.

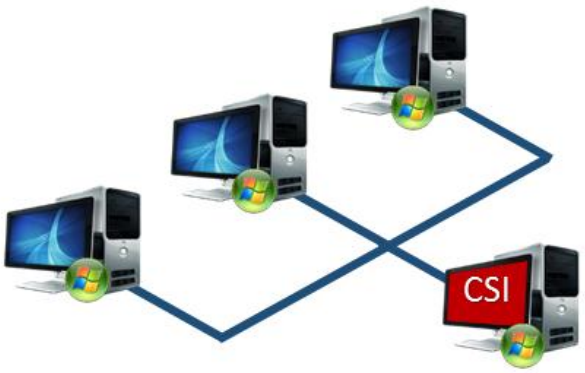
# Remote Scanning Via CSI (Agent-less Scan)

The following options are listed under **Scanning**:

- Quick Scan
- Scan Groups
- Scan Progress
- System Center Configuration Manager Inventory Import

Use these options to perform and monitor the progress of scans conducted on your PC and/or remote hosts on your network.

These scans are performed in an Agent-less manner and the credentials used by the Secunia CSI to authenticate on the target hosts will be the same as those of the user that launched the Secunia CSI console.




⚠ Please consider the system requirements for the Scan Groups/Agent-less scans, described in Remote/Agent-less Scan – Requirements (Windows).

# Quick Scan

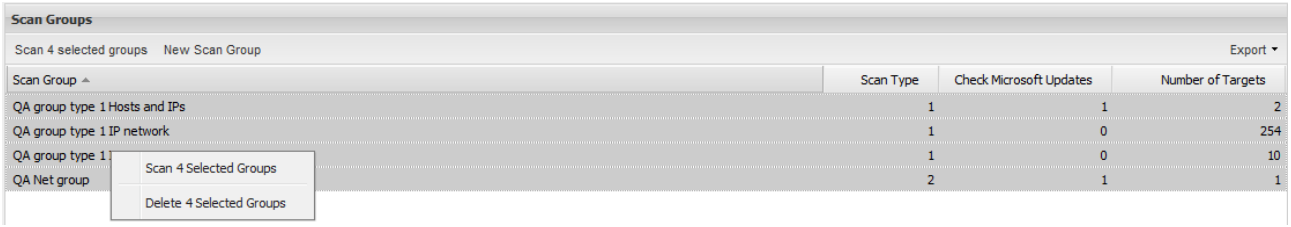
Use this page to conduct quick, on-demand, scans from your Secunia CSI console against remote hosts on your network or your local PC. Enter the scan type and IP address range for the hosts you wish to scan in the **Enter hosts to scan** screen and click **Scan Hosts**.

In order to make sure that you are able to remote scan the target host, please ensure that all the system requirements for the remote scan are in place.

The progress can be seen under **Scan Progress**.

# Scan Groups

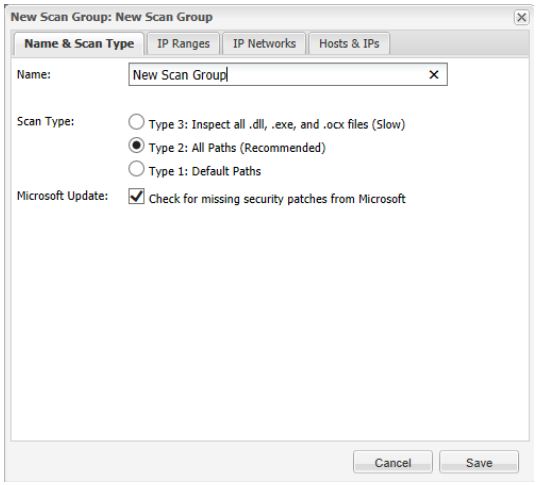
Use this option to create **Scan Groups** by choosing which hosts you would like to scan.


Scan Groups
Scan 4 selected groups
New Scan Group
Export
Scan Group
Scan Type
Check Microsoft Updates
Number of Targets
QA group type 1 Hosts and IPs 1 1 2
QA group type 1 IP network 1 0 254
QA group type 1 1 0 10
QA Net group 2 1 1
Scan 4 Selected Groups
Delete 4 Selected Groups

Click **New Scan Group** to create and configure a group of hosts to be scanned.

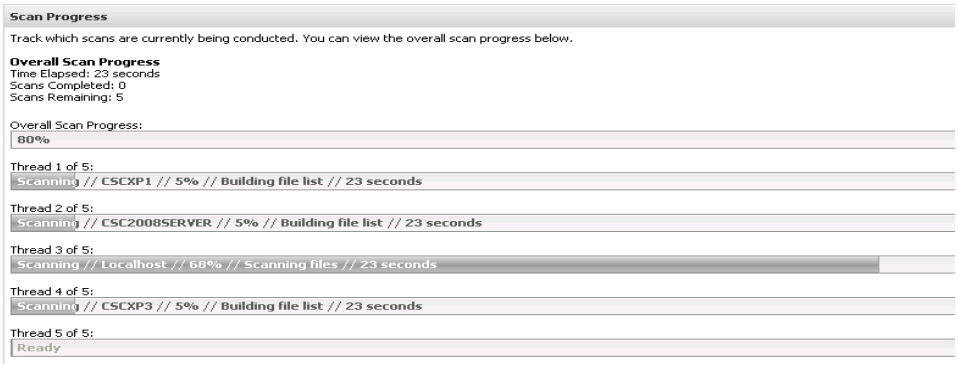
After navigating through the different tabs: **Name & Scan Type**, **IP Ranges**, **IP Networks** and **Hosts & IPs**, click **Save** to save and create the scan group.

To start a scan on a previously created group, right-click the group name and select **Scan Group**.




# Scan Progress

Use this page to track the scans being conducted. You can also configure the number of simultaneous scan threads (the default value is set to 5) as described in Scan Settings.


Scan Progress
Track which scans are currently being conducted. You can view the overall scan progress below.
Overall Scan Progress
Time Elapsed: 23 seconds
Scans Completed: 0
Scans Remaining: 5
Overall Scan Progress:
80%
Thread 1 of 5:
Scanning // CSCXP1 // 5% // Building file list // 23 seconds
Thread 2 of 5:
Scanning // CSC2008SERVER // 5% // Building file list // 23 seconds
Thread 3 of 5:
Scanning // Localhost // 68% // Scanning files // 23 seconds
Thread 4 of 5:
Scanning // CSCXP3 // 5% // Building file list // 23 seconds
Thread 5 of 5:
Ready

# System Center Configuration Manager Inventory Import

Use this page to scan and display hosts connected to the upstream System Center Configuration Manager. Scan results are obtained from the data collected by the System Center Configuration Manager software inventory agent, which avoids the need to install the Secunia CSI agent on each client. To be able to detect missing Microsoft security patches then you will need a connection to your Software Update Point (**Patching > Configuration > WSUS/SCCM (Connected)**) otherwise the scan will be Partial.

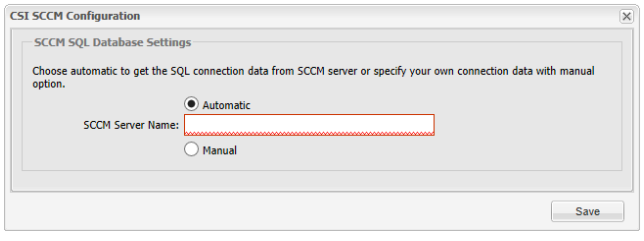
The System Center Configuration Manager software inventory agent must be configured and running prior to loading the System Center Configuration Manager inventory page. The inventory agent is configured by a set of simple rules that govern which files are queried. To produce the best possible scan result using System Center Configuration Manager, the Secunia CSI uses a relatively broad pattern, which could lead to large amounts of data being collected. If all file data is collected, a file size of between 5 and 10 MB for a single host is not uncommon, and the SQL server must be dimensioned to handle this.

System Center Configuration Manager integration requires the following prerequisites:

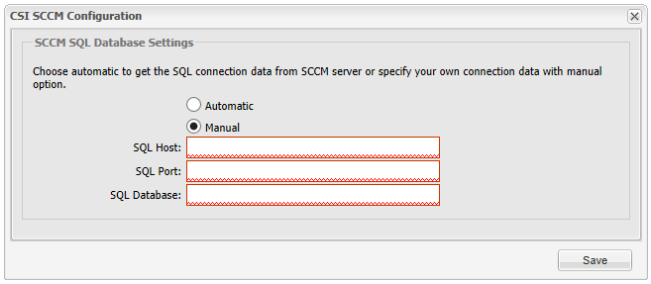
1. **Setting up authentication.** The user running the CSI console must have access to the database containing the data of the System Center Configuration Manager. For System Center 2012 Configuration Manager the database is named **CM_<site_code>** and for System Center Configuration Manager 2007 it is named **SMS_<site_code>.** To add permissions, open SQL Server Management Studio, right-click the appropriate database, navigate to permissions and add Connect and Select rights.
2. **Setting up the software inventory agent.** Assuming that the System Center Configuration Manager site has been set up, open the System Center Configuration Manager console and ensure that the System Center Configuration Manager client (agent) is installed on the hosts to be scanned. In System Center 2012 Configuration Manager, go to **Devices** and right-click **Install client**. Then go to **Administration > Client Settings > Properties > Software Inventory**. To configure the broadest possible pattern, select **File Detail: full** and add the patterns *.dll, *.exe, *.ocx. Do not exclude the Windows directory. Less data will be generated by specifying a narrower pattern, however, the quality of the scan result will suffer.
3. In addition, you might want to consider increasing the software inventory file size from the default of 5 MB to 12 MB. To accomplish this, change the following registry key on the System Center Configuration Manager Server:

   *HKLM\Software\Microsoft\SMS\Components\SMS_SOFTWARE_INVENTORY_PROCESSOR\Max File Size*

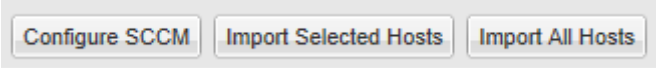
Click **Configure SCCM**. In the CSI SCCM Configuration page, enter the **SCCM Server Name** and click **Save**.


CSI SCCM Configuration
SCCM SQL Database Settings
Choose automatic to get the SQL connection data from SCCM server or specify your own connection data with manual option.
Automatic
SCCM Server Name:
Manual
Save

If you select **Manual**, enter the SQL Host, SQL Port and SQL Database connection data and click **Save**.


CSI SCCM Configuration
SCCM SQL Database Settings
Choose automatic to get the SQL connection data from SCCM server or specify your own connection data with manual option.
Automatic
Manual
SQL Host:
SQL Port:
SQL Database:
Save

In the System Center Configuration Manager Inventory Import page, click **Import Selected Hosts** or **Import All Hosts**.




⚠ Installing the System Center Configuration Manager client for the first time on a host can be time consuming and, in most cases, patience is required.

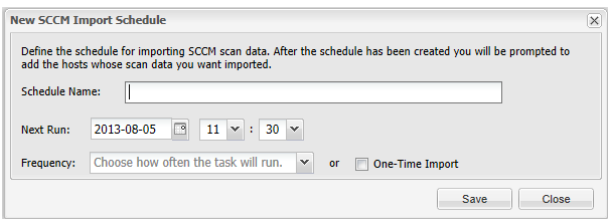
⚠ The scan result is based on the data collected by the software inventory agent, which may not be of the same quality as that of the Secunia CSI agent. This means that there could be discrepancies between a scan performed by the System Center Configuration Manager integration and the csia. It may also result in some products not being detected correctly. For higher quality scan results Secunia recommends using the csia.

## System Center Configuration Manager Import Schedules

Use this page to create and maintain System Center Configuration Manager Import Schedules.

Click **New SCCM Import Schedule** and enter:

- The **Name** of the import schedule
- The **Next Run** date and time
- The **Frequency** (Hourly, Daily, Weekly or Monthly) that the import will be performed or select the **One-Time Import** check box


New SCCM Import Schedule
Define the schedule for importing SCCM scan data. After the schedule has been created you will be prompted to add the hosts whose scan data you want imported.
Schedule Name:
Next Run:
2013-08-05
11
30
Frequency:
Choose how often the task will run.
or
One-Time Import
Save
Close

Click **Add Hosts** and enter the **Domain** and **Host** to include in the Import Schedule.

Right-click an Import Schedule in the grid to edit or delete the schedule.

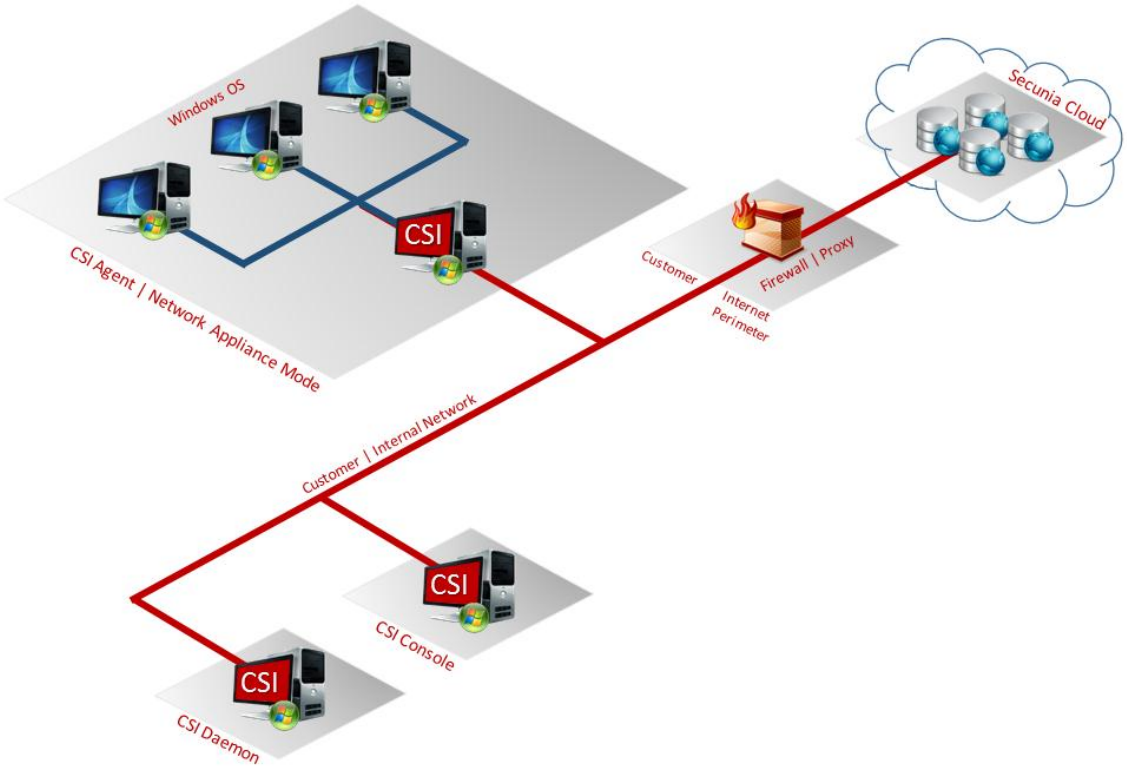
# Remote Scanning Via Agents

You can use Network Appliance Agents for scanning one or more networks at scheduled intervals without having to install the Secunia CSI Agent in every single target host.

With the csia.exe installed in Network Appliance mode, you will have the ability to schedule remote scans.

The hosts to be scanned can be identified by an IP-range, IP-network or Host-name.

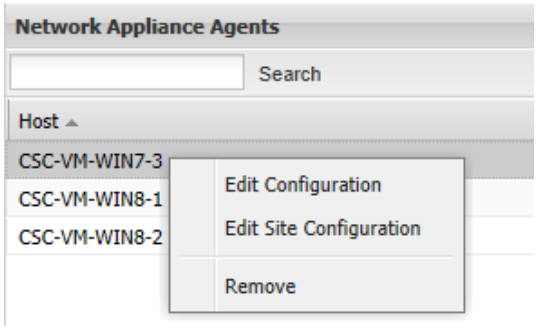
The CSI console allows you to easily manage the scans being performed by the Network Appliance Agent.




⚠ Please consider the system requirements for the Scan Groups/Agent-based scans, described in Agent-based Scan – Requirements (Windows) and Agent-based Scan – Requirements (Mac OS X).

## Network Appliance Agents

Use this page to view a list of the hosts which have Network Appliance Agents installed. Right-click a host to configure the Network Appliance Agent installed on that host.




To scan using a Network Appliance Agent you must:

- Install the agent in Network Appliance mode
- Create a Network Appliance Scan Group

A schedule links the above to perform scans of the group at set intervals.

## Network Appliance Groups

Use this page to create a target group that will be scanned by a Network Appliance Agent. Click **New Group** to create a new target group that will be remotely scanned by one of the Network Appliance Agents previously installed.

## Download Network Agent

Use this page to download the csia.exe file as well as read an explanation on how to install the Network Appliance Agent.

> ⚠ Ensure that the Agent file csia.exe is available in the system that will host the Agent in Network Appliance mode.

**Example:** If you want to scan three different networks (for example Germany, United States, and United Kingdom) without having to install the Agent in Single Host mode, then you can install three instances of csia.exe in Network Appliance mode, one on each network.

Afterwards you will be able to scan all the hosts on the three locations at scheduled intervals by creating the appropriate scan groups in **Network Appliance Groups** and assigning each group to its respective and previously installed Network Appliance Agent.

**Result:** 15 minutes after installing a csia.exe in Network Appliance mode, the Network Appliance Agent will appear in **Scanning > Remote Scanning Via Agents > Network Appliance Agents**.

To specify the target host to be scanned by the Network Appliance Agent, please configure the scan group in **Scanning > Remote Scanning Via Agents > Network Appliance Groups**.

Installing the Network Appliance Agent from the command prompt:

**>csia.exe -A –i**

It is essential that the csia.exe is installed with the correct credentials.

The user installing the Network Appliance Agent must have admin rights to all the target hosts that will be scanned by the Network Appliance Agent.

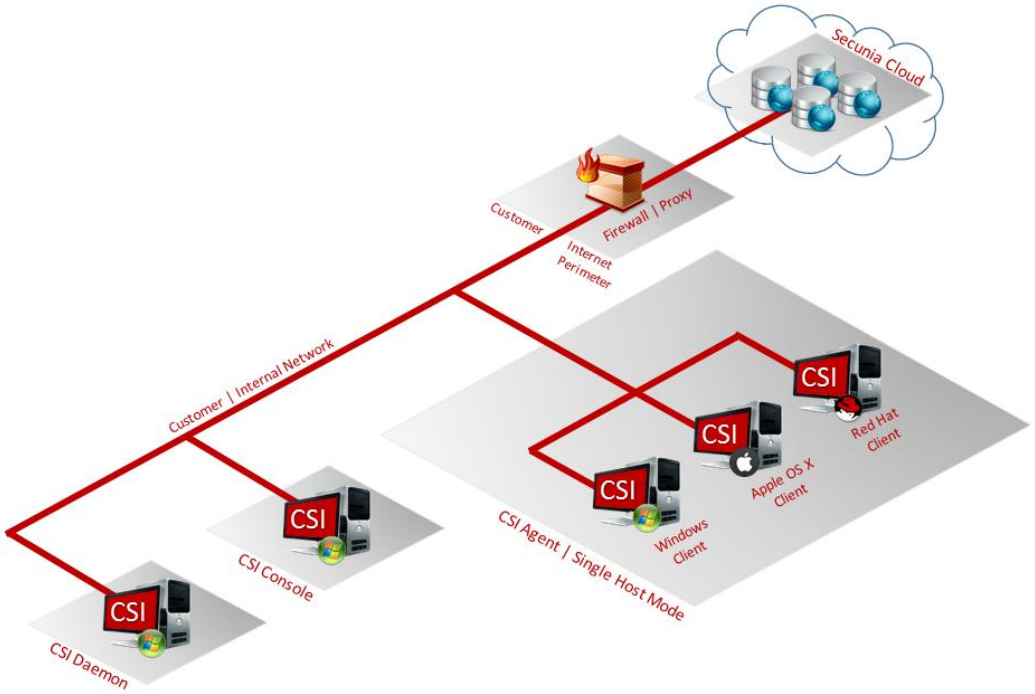
Example of an installation:

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>cd "\Program Files\Secunia\CSI"

C:\Program Files\Secunia\CSI>csia.exe -A -i
Enter password for user 'Administrator':
Starting 'Secunia CSI Agent' service
'Secunia CSI Agent' service started
'Secunia CSI Agent' successfully installed

C:\Program Files\Secunia\CSI>
```

## Scanning Via Local Agents

The Secunia CSI provides different scan approaches, enabling you to select the one that best suits your environment. The Agent-based deployment is more robust and flexible for segmented networks or networks with mobile clients (for example, laptops). Once installed, the Agent will run silently in the background.

This is the recommended scanning approach due to its flexibility, usage convenience, and performance.




⚠ Please consider the system requirements for the Scan Groups/Agent-based scans, described in Agent-based Scan – Requirements (Windows) and Agent-based Scan – Requirements (Mac OS X).

## Single Host Agents

Use this page to manage configurations and schedule scans for the hosts where the Agent is installed as a service in Single Host mode.

Double-click a host to manage the configuration of the selected Agent and change its settings (Inspection type, Check-in frequency, Days between scans).

Right-click a host name and select **Edit Site Configuration** to manage the configuration for all the hosts in that Site.

The hosts scanned with the csia.exe will be grouped by Site. By default the domain name will be used as a Site name.

To change a Site name, please refer to Sites. You can also specify a Site name when installing the Agent, by using the **-g** parameter or by specifying a site name in the additional parameters when creating the Agent deployment package described in Agent Deployment.

## Download Local Agent

Use this page to download the csia.exe file as well as read an explanation on how to install the Secunia Agent in Single Host mode.

If your intention is to deploy the Secunia CSI Agent through WSUS/System Center Configuration Manager please refer to Agent Deployment for further information.

> ⚠ Ensure that the Agent (csia.exe) is available in a local folder on the target PC before installing.

**Example:** Install the csia.exe (Agent) in Single Host mode; download the Agent from the CSI console under **Scanning > Scanning via Local Agents > Download Local Agent**.

Once the Agent is installed, every time, for example, the laptop goes online (Internet connection) it will verify if a new scan should be conducted.

After scanning, the result will be displayed in **Scanning > Completed Scans** in the Secunia CSI console.

> ⚠ When the Secunia CSI Agent is installed a unique identifier is generated so that each Agent has its own unique ID. For this reason, the Agent should not be included in OS images. Doing so will result in having several instances of the same Agent and in the inability to correlate the scan results with the scanned hosts.

**Result:** Hosts scanned with the Agent in Single Host mode will be displayed in **Results > Host Smart Groups**.

When and how the hosts are scanned can be controlled from the Secunia CSI console under **Single Host Agents**. Right-click a host name and select **Edit Configuration** to change the Agent settings.

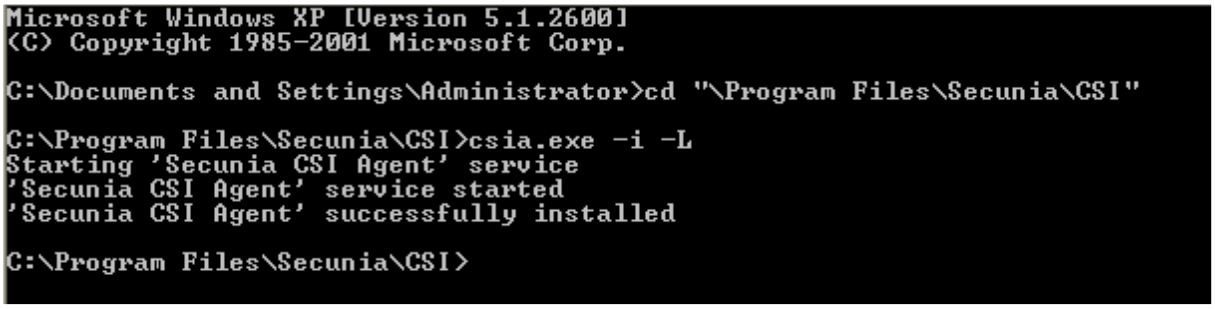
⚠ Install the Agent from the command prompt with local Admin account using:
**>csia.exe -i -L**

By using the **-L** parameter, the Agent will be installed as a service running under the LocalService user account. For further information, refer to:
http://msdn.microsoft.com/en-us/library/windows/desktop/ms684190%28v=vs.85%29.aspx

If you are a member of a domain and you do not use the **-L** switch, the service will be installed under the user account performing this action, granting the 'logon as a service' privilege.

However, this privilege is usually removed in the next GPO background refresh since domain policies will not allow it. As a consequence, the Agent will stop working after the privilege has been removed.

Example of an installation:


Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Administrator>cd "\Program Files\Secunia\CSI"
C:\Program Files\Secunia\CSI>csia.exe -i -L
Starting 'Secunia CSI Agent' service
'Secunia CSI Agent' service started
'Secunia CSI Agent' successfully installed
C:\Program Files\Secunia\CSI>

Refer to Agent Deployment to deploy the csia.exe through WSUS/System Center Configuration Manager for further information of how to deploy the csia.exe via Group Policy.

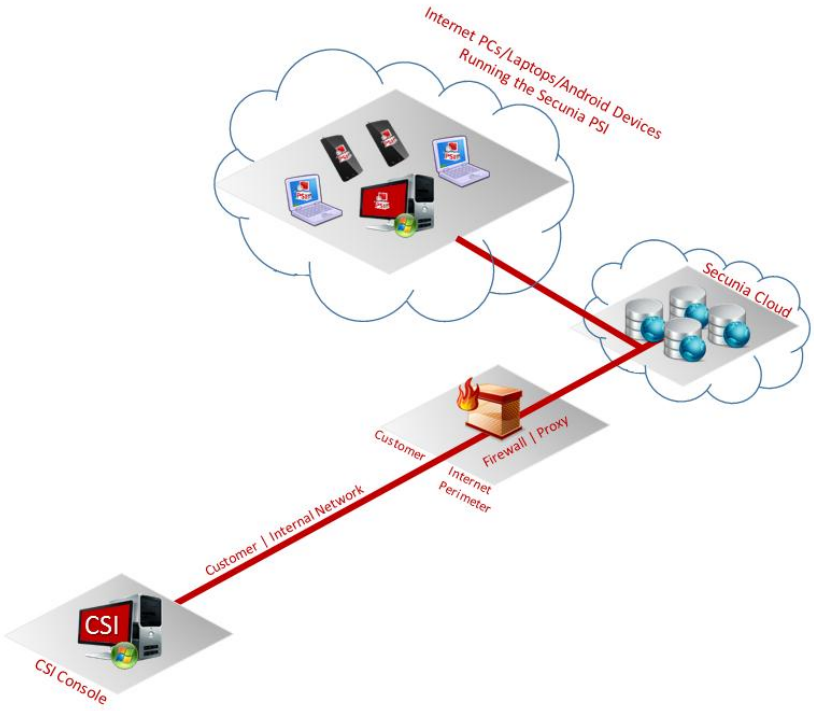
⚠ The csia.exe file is a customized executable, unique and private for your Secunia CSI account. This means that the csia.exe automatically links all scan results to your Secunia CSI account.

# PSI for Windows and Android

## PSI for Windows

The Secunia Personal Software Inspector (PSI) offers integration with the Secunia CSI 7.0, making it possible to view PSI scan results and approve patches from the Secunia CSI console. This enables an administrator to track all the unmanaged PCs/Laptops/Android Devices connecting to the network and take any remediation actions necessary.

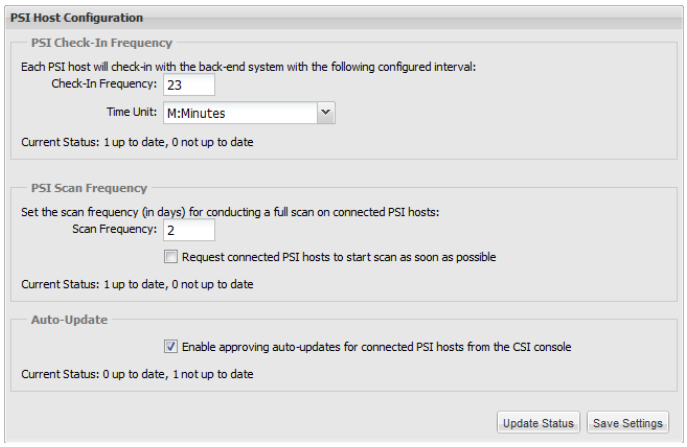
The Secunia PSI results are hosted in the Secunia Cloud and fetched from there by the Secunia CSI console.




## Host Configuration

Use this page to centrally manage the configuration settings of all Secunia PSI connected installations.

All configuration settings available in this page will be applied to the connected PSI installations.


PSI Host Configuration
PSI Check-In Frequency
Each PSI host will check-in with the back-end system with the following configured interval:
Check-In Frequency: 23
Time Unit: M:Minutes
Current Status: 1 up to date, 0 not up to date
PSI Scan Frequency
Set the scan frequency (in days) for conducting a full scan on connected PSI hosts:
Scan Frequency: 2
Request connected PSI hosts to start scan as soon as possible
Current Status: 1 up to date, 0 not up to date
Auto-Update
Enable approving auto-updates for connected PSI hosts from the CSI console
Current Status: 0 up to date, 1 not up to date
Update Status
Save Settings

⚠ The PSI Host Configuration settings are not continuously kept in tight synchronization. As a consequence some hosts may become out of sync with the settings displayed here, for example newly added hosts, and PSI users with local administration rights may change the settings locally.

For more detailed information regarding the Secunia PSI, please visit:

https://secunia.com/vulnerability_scanning/personal/

## Configure Link ID

Use this page to download the custom Secunia PSI 3.0 setup file. Please note that your Link ID will be part of the filename and must not be changed.

You can then install the Secunia PSI using the downloaded installer on the target host and perform a scan on the target host using the Secunia PSI.

The target host will then be listed in the **Results > Host Smart Groups > Configured Host Groups** page of your Secunia CSI console.

⚠ Changing the Link ID will break the link between your Secunia CSI account and all Secunia PSI users that are currently configured to use the existing Link ID.

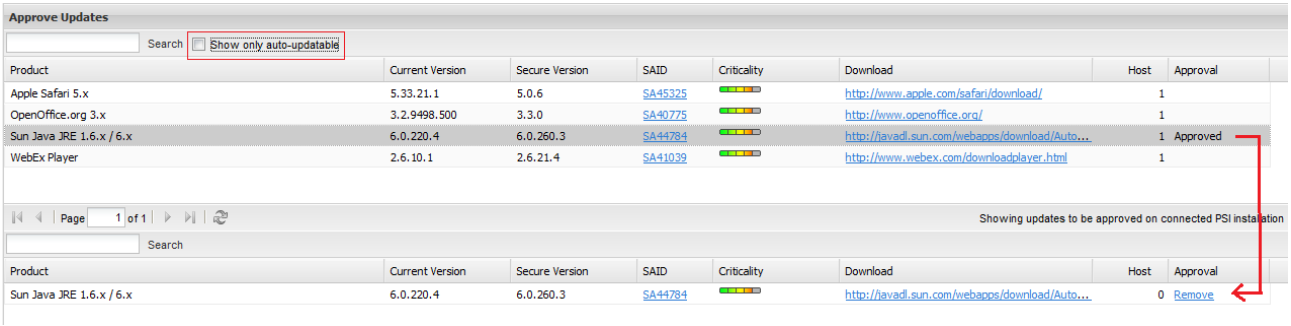
## Approve Updates (for Connected PSI Installations)

Use this page to view the list of Insecure and End-Of-Life software on connected PSI installations.

Click **Approve** to apply updates that can automatically be applied without interaction with the PSI user.

Once an update is approved it will be shown in the bottom grid.

Any PSI host being added later will receive updates that have been approved in the past (if applicable).




The products which are already approved by the CSI administrator will be displayed in the lower pane.

⚠ Approving an update in the CSI does not trigger the PSI to perform any action. The PSI will not pick up the action until a new scan is triggered, the system is restarted, and so on. The Secunia PSI will download the updates/patches from the link suggested by Secunia (usually by the vendor of the product being patched that hosts the update). The Secunia PSI does not connect to WSUS or SCCM.

## PSI for Android

The Secunia PSI for Android is a free security scanner that allows a user to scan their mobile device and detect any vulnerable products installed.

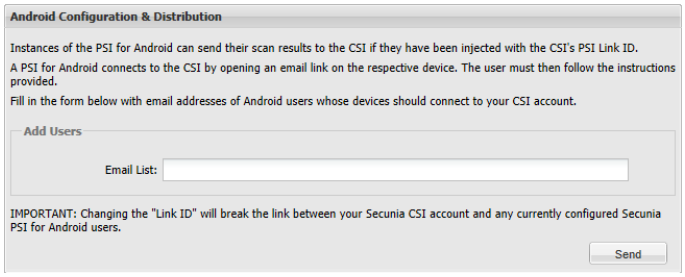
After examining all the products on a user's mobile device, the collected data is sent to Secunia's servers, which match the data against the Secunia File Signatures engine to determine the exact applications installed on their device.

The Secunia PSI for Android supports Android OS versions from 2.2 onwards.

The Secunia PSI for Android users can connect to the Secunia CSI by opening the PSI Link ID that has been sent to them by email from the Secunia CSI user and following the instructions provided.

## Configuration and Distribution

Use this page to add the email addresses of PSI for Android users whose devices should connect to your CSI account.


Android Configuration & Distribution
Instances of the PSI for Android can send their scan results to the CSI if they have been injected with the CSI's PSI Link ID.
A PSI for Android connects to the CSI by opening an email link on the respective device. The user must then follow the instructions provided.
Fill in the form below with email addresses of Android users whose devices should connect to your CSI account.
Add Users
Email List:
IMPORTANT: Changing the "Link ID" will break the link between your Secunia CSI account and any currently configured Secunia PSI for Android users.
Send

⚠ Changing the Link ID will break the link between your Secunia CSI account and any currently configured Secunia for PSI Android users.

# Scanning Mac OS X

To scan Apple Mac OS X machines, you need to deploy the Single Host Agent locally on the target system.

The installation can only be done under the MAC Terminal, as the agent will be installed as a daemon (service) under the LocalSystem account.

Installation of Local Services on MAC OS X systems requires root privileges. The 'root' account is disabled by default on MAC systems; therefore you need to enable it in order to proceed.

## Download the CSIA for Apple Mac OS X

The Secunia CSI Agent for MAC OS X (csia) is a small, simple, customizable and extremely powerful Secunia CSI scan engine that offers a fully featured command line interface (CLI) to the Secunia CSI scanning functionality.

This allows you to run CSI scans directly from the command line, or to launch scans by using the Secunia CSI console.

You can download the agent binary under **Scanning > Scanning via Local Agents > Download Local Agents**.

⚠ Ensure that the agent is always available in a local folder on the target host.

## Prepare Your MAC

Installation of daemons (services) on MAC OS X systems requires **root account** privileges. This means that root account should always be used when installing the Secunia CSI Agent.

You can switch to your local root account by using the command '***su root***' in your Mac Terminal. You will be prompted to provide the password for the root account.

```
bash-3.2$ su root
Password:
```

Provide the password for '**root**' if you know it. If you are not certain about the password, you may want to try entering '**toor**', which is the default password for the root account, or you may also try with the current password of your Administrator account. Both ways may work, but if the account is disabled on the system, none of the passwords would work.

⚠ The Terminal window will not display the password you typed in. Once you have entered the password correctly, press ENTER and wait for confirmation.

If you do not know the password for the root account, or the latter is currently disabled, you can perform the following actions in order to enable the account and set a new password:

- Open **Terminal**
- Type ***sudo passwd root***
- Provide a new password

For more details on how to enable root account on MAC OS X systems, please refer to: http://support.apple.com/kb/ht1528

⚠ If you cannot enable the '**root**' account on the MAC, or you prefer to not use it directly, you can alternatively use the '**sudo'** switch before each command associated with Agent activities. For example: '***sudo ./csia –i –L'*** can be used to install the Agent on the system.

Once you are ready with setting/logging the root account you are one step away from installing the Agent.

When you download the Agent on a MAC system, normally the file is being set with limited file permissions on the system. You must check whether the file is allowed execution on the system by using the '**ls -l**' command which will list the file and will show its file permissions.

```
-rwxrwxrwx  1 csc  staff  803460 May 30 11:04 csia
-rwxr-xr-x@ 1 csc  staff  803460 Jun 11 13:04 csia_csc50
```

In case the permissions do not include execute rights (the '**x**' character) for any user, you should set them for at least the root/Administrator account by using the ***chmod +x*** command.

- ***chmod +x csia*** (If you are using the Administrator account, add **sudo** before **chmod**)

## Install MAC Agent

The traditional way of installing the Secunia CSI Agent is as a daemon (similar to local service in Windows) as it will operate under the MAC OS X LocalSystem account. Install the binary by using the MAC Terminal services in the following way:

- Open **Terminal**
- **Browse** to the directory where you have placed the csia binary file
- **Type** the following command to install the agent: ***./csia –i –L***

```
sh-3.2# cd /Users/secunia/Desktop/
sh-3.2# ./csia -i -L
[08/01 12:48:10.610] Initializing Secunia CSI Agent
[08/01 12:48:10.687] Installing service
```

The agent shows in the Secunia CSI console approximately 15 minutes after the installation.

To launch a new scan manually under the MAC Terminal, issue the command ***'. /csia –c'***

Use the ***'-h'*** switch to see a full list of parameters supported by the agent.

# Scanning Red Hat Enterprise Linux (RHEL)

Red Hat Enterprise Linux (RHEL) 5 and 6 are the only operating systems officially supported by Secunia for the CSI RHEL scan agent. It may be possible to install the scan agent on operating systems and configurations other than those described. However, these have not been tested and are not supported by Secunia.

The scan agent for RHEL uses the inventory which is already present (RPM) and displays this in the Secunia CSI after being processed by Secunia Detection/Version Rules. To download the Secunia CSI Agent for Red Hat Linux, go to **Scanning > Scanning via Local Agents > Download Local Agents**.

## Installing the CSIA for Red Hat Linux

> ⚠ Please note that this is a sample reference implementation that you can use to help guide your setup.

**To install the CSIA for Red Hat Linux:**

Login as root at the RHEL machine and install/update the package (the same command line option works for both cases):

```
su root
/bin/rpm -U <path>/csia_linux-7.0.0.11-1.noarch.rpm
```

**Specifying proxy settings for the scanner (recommended method):**

Set the applicable standard proxy environment variables from this set:

```
no_proxy
NO_PROXY
https_proxy
HTTPS_PROXY
http_proxy
HTTP_PROXY
all_proxy
ALL_PROXY
```

Alternatively, you can update the proxy setting to override the environment variables:

1. Update the proxy setting in the configuration file `/etc/csia_config.xml`
2. Login as root and restart the scanner service:

```
su root
service secunia_csia restart
```

**Specifying the LAN Group of the machine:**

This setting will be overridden if the DNS domain name of the machine is publicly available (check with the 'dnsdomainname' command).

1. Update the lanGroup setting in the configuration file `/etc/csia_config.xml`
2. Login as root and restart the scanner service:

```
su root
service secunia_csia restart
```

**Immediately update the RHEL Agent configuration:**

If you have set the agent check-in time to, for example, 1 day, it will be 1 day until the RHEL Agent picks up any configuration changes. If you want the RHEL Agent to immediately adapt to configuration changes, you can use the commands below to accomplish this by simply restarting the Agent service.

Login as root and restart the scanner service:

```
su root
service secunia_csia restart
```

**Uninstalling:**

Login as root and uninstall the scanner RPM package:

```
su root
/bin/rpm -e csia_linux-7.0.0.11-1.noarch
```

# Filter Scan Results

Use this page to filter scan results, either by restricting/allowing the scanning to specific paths or by creating Smart Groups that scan only the products you specify.

## Scan Paths

Use this feature to create either a Whitelist or Backlist of paths/locations to restrict the locations inspected by the Secunia CSI scan.

Click **Add Whitelist Rule** or **Add Blacklist Rule** and enter the **Name**, **Path** and **Site (optional)** details.

> ⚠ This feature is not applicable to Mac OS X, RHEL or PSI.

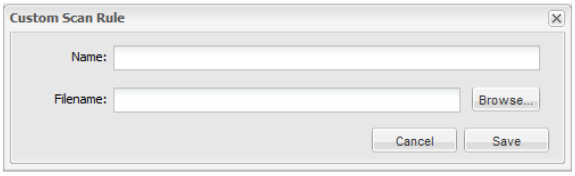
If using the Whitelist, all the locations white-listed will be inspected by the scanner and any other locations are excluded from the Secunia CSI inspections.

If using the Blacklist, all the locations/paths black-listed will be ignored and any other paths are inspected by the Secunia CSI scan.

> ⚠ Use this feature with **caution.** By using the Scan Path Rules some of your paths will be excluded from the scan and the Secunia CSI will not alert you towards excluded insecure products, even if they potentially expose your hosts to security threats.
>
> It is not possible to simultaneously use both a Blacklist and a Whitelist.

## Custom Scan Rules

Use the Custom Scan Rules page to create and maintain custom rules for scanning customer created programs, drivers, and plugins. Click **New Custom Scan Rule** and enter a **Name** for the rule and the **Filename** to scan. You can also click **Browse** to search for the file you want to add to the rule.

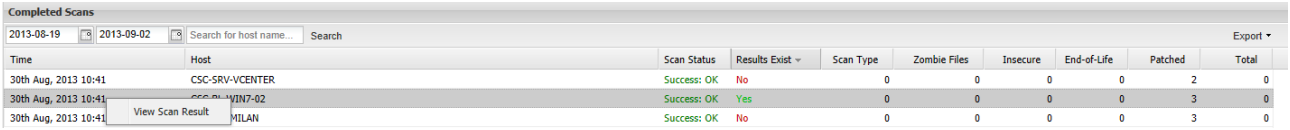


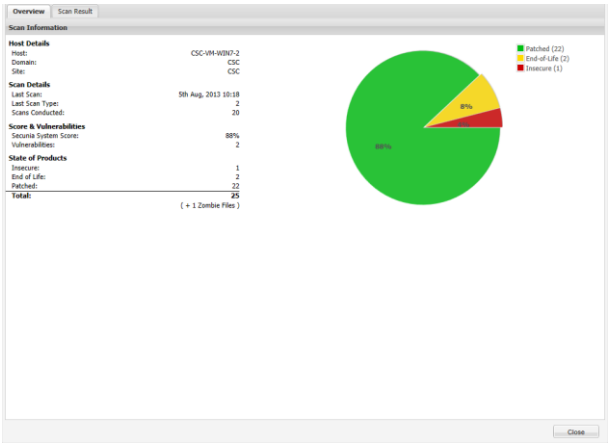

Right-click a rule in the grid to edit or delete the rule.

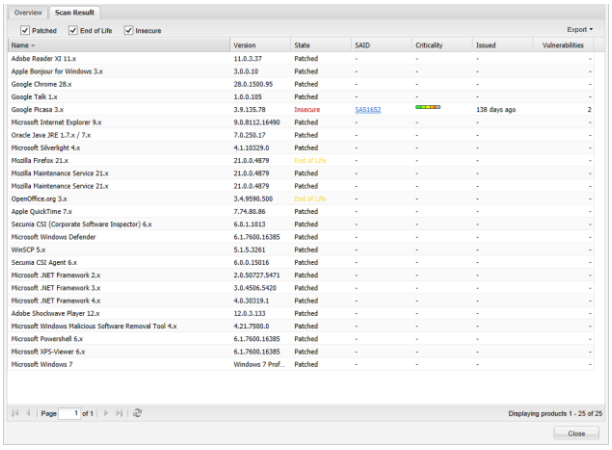
> ⚠ The file to be scanned must contain valid File Version Information.

# Completed Scans

Use this page to view a summary of the scans conducted. Double-click an entry for which results exist for further details or right-click and select **View Scan Result**.




**Scan Status:**

**Success** – The scan was completed successfully.

**Partial** – The Secunia CSI scans consists of 2 parts; the first part is the scan of third-party applications, the second part is collecting information about Microsoft patching status from the Windows Update Agent (WUA).

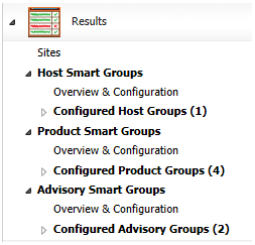
If the Secunia CSI scan engine is not able to obtain the required information from the WUA, the scan result will be **Partial**. If you need to troubleshoot why the scan result is partial, please consider the following:

- http://msdn.microsoft.com/en-us/library/aa387288%28v=vs.85%29.aspx
- Check the setting that controls the behavior of the WUA when a scan is completed (refer to Settings for further information)

**Failed** – The Secunia CSI was not able to connect to the remote target in order to perform the scan. Refer to Remote/Agent-less Scan – Requirements (Windows) for further information.

# Results

## Sites




Use this page to view the Sites maintained within your account. You can double-click a Site name to see all the hosts grouped under that Site name.

Right-click a Site to view its Hosts or delete the Site.

Scanned hosts will be grouped in a Site with the same name as the domain they log on to.

⚠ Switching to Active Directory will remove your current Sites structure (your existing data will be backed up).

## Smart Groups

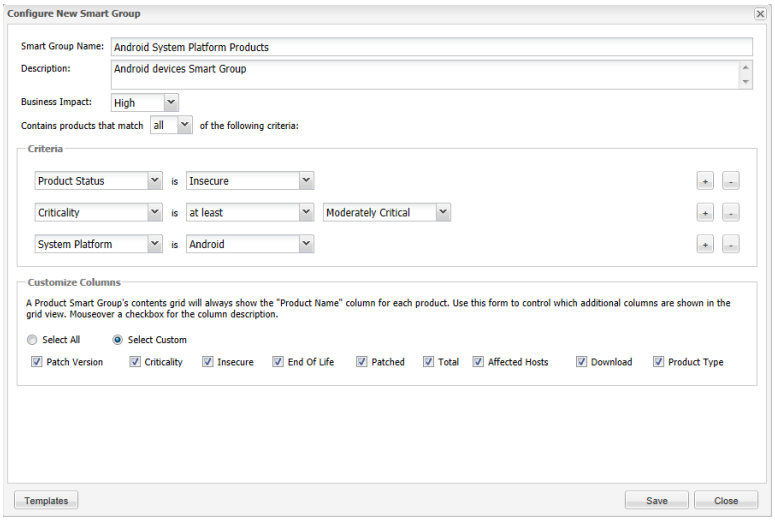
Smart Groups are the medium by which a CSI user views scan results. You are able to see the hosts, products, and associated advisories that are available to you, based on your view of the network as configured by your administrator. Furthermore, you are able to create custom filtered views of each of these using a variety of pre-defined criteria. The **All Hosts**, **All Products**, and **All Advisory** default Smart Groups are created by Secunia, and cannot be edited or deleted. They represent an unfiltered view for their respective content. Use the filters when creating additional Smart Groups to effectively customize the data you are most interested in, and want to see, create reports on, receive alerts and notifications about, and see dashboard portlet data on. Smart Groups are the basis by which most data in the CSI is viewed, and can be used effectively to optimize your workflow.

Note that Smart Groups are generated periodically, and the data you see is only as current as the last time the Smart Group was compiled. At any time you can queue the recompilation of a Smart Group to get the most current data.

Within the Smart Group grids, you can double-click to view/edit an existing group's configuration. Alternatively, right-click a Smart Group to view, edit, compile or delete the group.

Select a Smart Group and click **Queue For Compilation** to update the data and notifications for the group. The group will usually update within minutes.

Click **Create New Smart Group** to configure a new Smart Group. Click **+** and **–** to add or remove criteria.




Click **Templates**, where available, to open the Smart Group Example Use Cases page. Select an appropriate use case and click **Use Template** to populate the Smart Group Overview and Configuration page, which you can then edit to match your specific requirements.

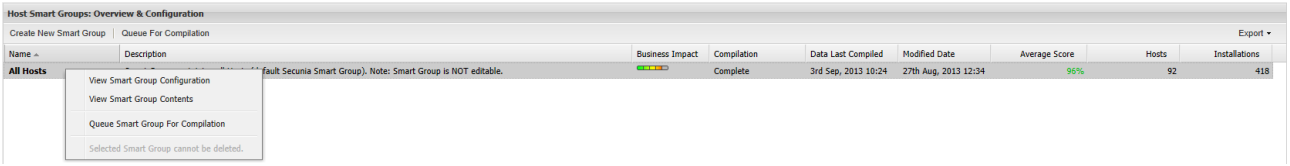
⚠ If you edit a configured Smart Group, all existing log files and notifications for the Smart Group will be deleted. New logs will be created after your changes have been saved.

⚠ Content can be available in multiple Smart Groups at the same time. For example, if you have a Smart Group showing all insecure products and another showing all products from Adobe, then if a host has an Adobe product installed that is insecure, this will be displayed in both Smart Groups. Also note that when you first run a scan you won't see the hosts in All Hosts, or any reports, until the Smart Group is compiled.

# Host Smart Groups

## Overview and Configuration

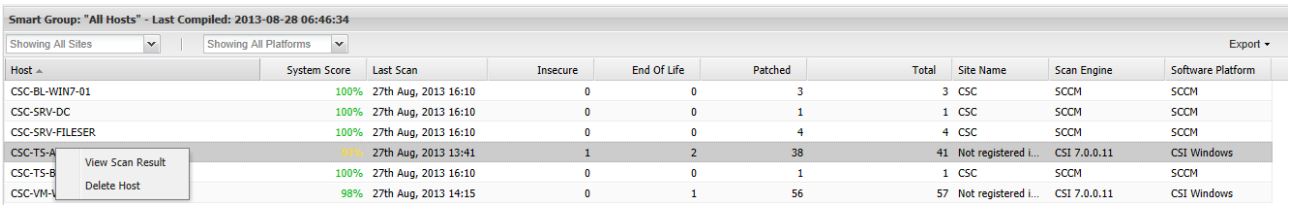
Use this page to view the existing configured Host Smart Groups and configure new Smart Groups. Right-click an item in the grid to view, edit, compile or delete the Smart Group.

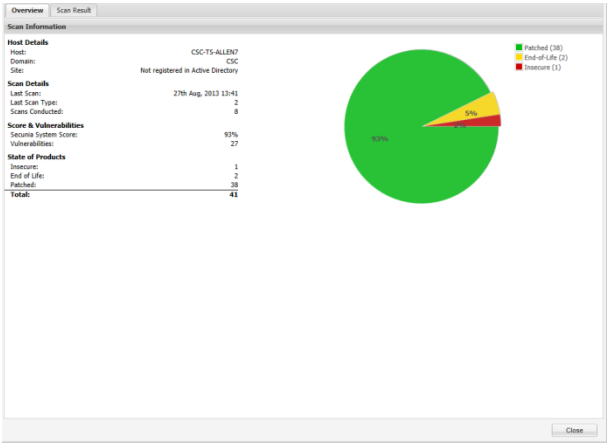


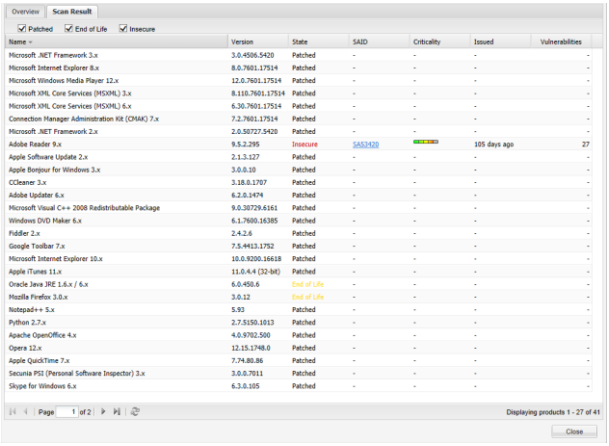

**All Hosts** is the default Smart Group which cannot be edited or deleted.

## Configured Host Groups

Use this page to view the information for each Host Smart Group you created. Right-click an item in the grid to view the scan result or delete the selected host.


Smart Group: "All Hosts" - Last Compiled: 2013-08-28 06:46:34
Showing All Sites
Showing All Platforms
Export
Host
System Score
Last Scan
Insecure
End Of Life
Patched
Total
Site Name
Scan Engine
Software Platform
CSC-BL-WIN7-01 100% 27th Aug, 2013 16:10 0 0 3 3 CSC SCCM SCCM
CSC-SRV-DC 100% 27th Aug, 2013 16:10 0 0 1 1 CSC SCCM SCCM
CSC-SRV-FILESER 100% 27th Aug, 2013 16:10 0 0 4 4 CSC SCCM SCCM
CSC-TS-A 93% 27th Aug, 2013 13:41 1 2 38 41 Not registered i... CSI 7.0.0.11 CSI Windows
CSC-TS-B 100% 27th Aug, 2013 16:10 0 0 1 1 CSC SCCM SCCM
CSC-VM-V 98% 27th Aug, 2013 14:15 0 1 56 57 Not registered i... CSI 7.0.0.11 CSI Windows
View Scan Result
Delete Host

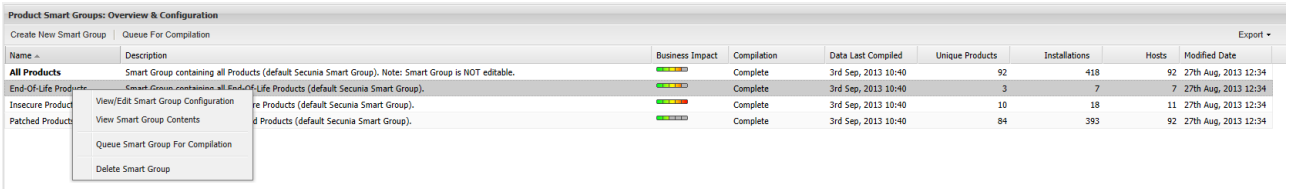


# Product Smart Groups

## Overview and Configuration

Use this page to view the existing configured Product Smart Groups and to configure new Smart Groups. Right-click an item in the grid to view, edit, compile or delete the Smart Group.

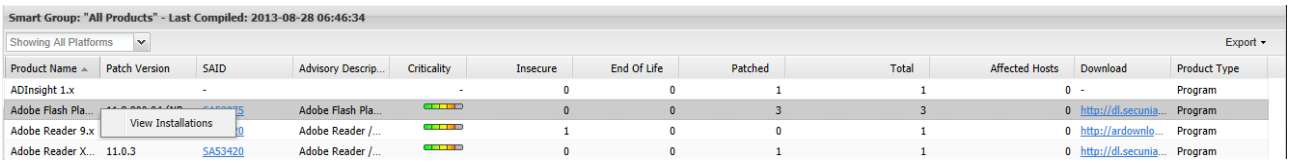


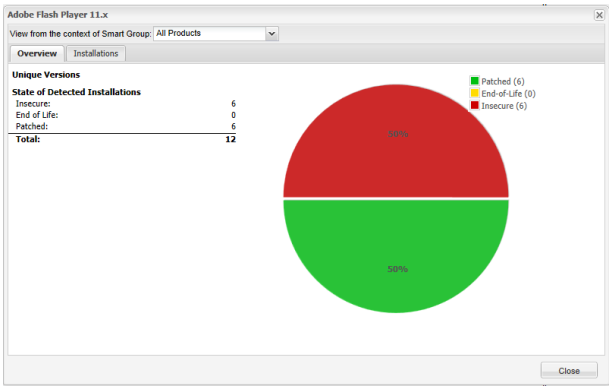

**All Products** is the default Smart Group which cannot be edited or deleted.

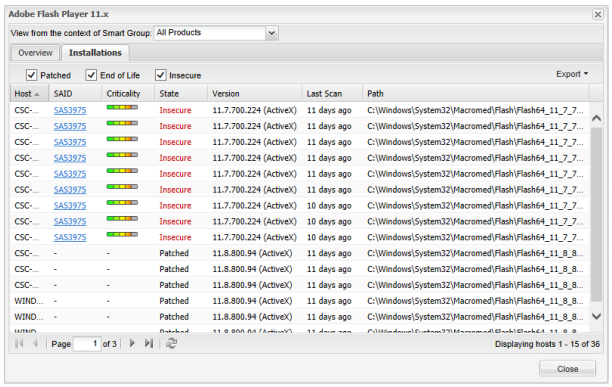
The other default Smart Groups for End-Of-Life Products, Insecure Products, and Patched Products have been pre-created for you by Secunia. You can right-click to view, edit, compile or delete these Smart Groups.

## Configured Product Groups

Use this page to view the information for each Product Smart Group you created. Right-click an item in the grid to display the installation details.



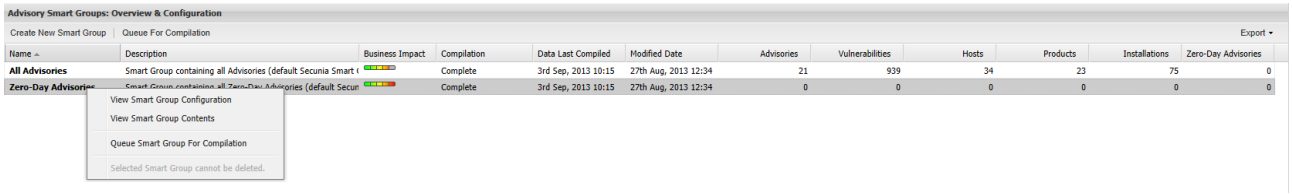



# Advisory Smart Groups

## Overview and Configuration

Use this page to view the existing configured Advisory Smart Groups and to configure new Smart Groups. Right-click an item in the grid to view, edit, compile or delete the Smart Group.




**All Advisories** is the default Smart Group which cannot be edited or deleted.

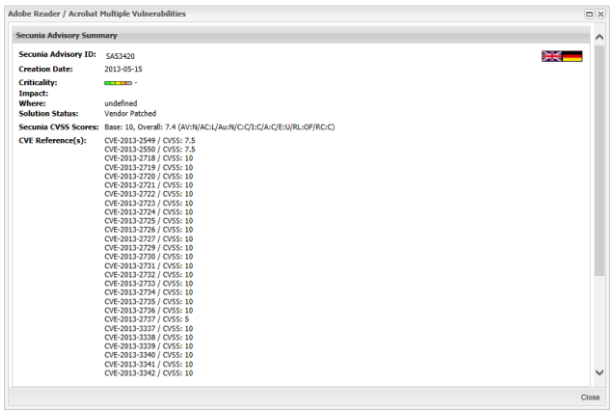
## Zero-Day Advisories (Optional Module)

A Zero-Day advisory is one for which, at the time of release, no patch exists, but an exploit does exist. That is to say, it is potentially being actively exploited by hackers, and there is no solution. If you subscribe to the Zero-Day Module, then you have a default non-editable Secunia-created Smart Group called Zero-Day Advisories which monitors any current Zero-Day advisories relevant to your software portfolio. Additionally, you are able to select Zero-Day Status as a filter criteria for your Advisory Smart Groups, so you can create additional filtered Smart Groups that incorporate this data.

# Configured Advisory Groups

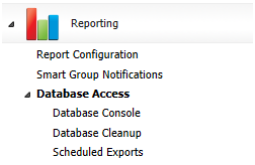
Use this page to view the information for each Advisory Smart Group you created. Double-click a Secunia Advisory ID (SAID) in the grid to display the details.

Smart Group: "All Advisories" - Last Compiled: 2013-07-29 07:13:16
Showing All Platforms
Export
SAID
Advisory Description
Criticality
Advisory Published
Vulnerabiliti...
Solution Status
CVSS Base Score
Installations
Products
Hosts
SA53975 Adobe Flash Player / AIR Multiple Vulnerabilities 9th Jul, 2013 0 Vendor Patched 10 12 1 6
SA53420 Adobe Reader / Acrobat Multiple Vulnerabilities 15th May, 2013 0 Vendor Patched 10 9 4 7
SA53894 Adobe Shockwave Player dir File Parsing Memory Corruption Vulnerability 9th Jul, 2013 0 Vendor Patched 10 2 2 1
SA53471 Apple iTunes Multiple Vulnerabilities 17th May, 2013 0 Vendor Patched 10 2 1 2
SA53520 Apple QuickTime Multiple Vulnerabilities 23rd May, 2013 0 Vendor Patched 10 3 1 3
SA47292 Apple Safari Multiple Vulnerabilities 10th May, 2012 0 Vendor Patched 10 1 1 1
SA41119 Camtasia Studio Insecure Library Loading Vulnerability 25th Aug, 2010 0 Partial Fix 9.3 1 1 1
SA30330 FileZilla GnuTLS Multiple Vulnerabilities 21st May, 2008 0 Vendor Patched 0 1 1 1
SA51733 Foxit Reader / PhantomPDF Plugin For Browsers URL Processing Buffer Overflow Vulnerability 8th Jan, 2013 0 Vendor Patched 10 1 1 1
SA54017 Google Chrome Multiple Vulnerabilities 9th Jul, 2013 0 Unpatched 10 7 2 6
SA48448 Google Talk Credentials Disclosure Security Issue 27th Mar, 2012 0 Vendor Patched 5 1 1 1
SA53976 IrfanView ANI File Processing Integer Overflow Vulnerability 5th Jul, 2013 0 Vendor Patched 10 3 1 3



# Reporting

## Report Configuration

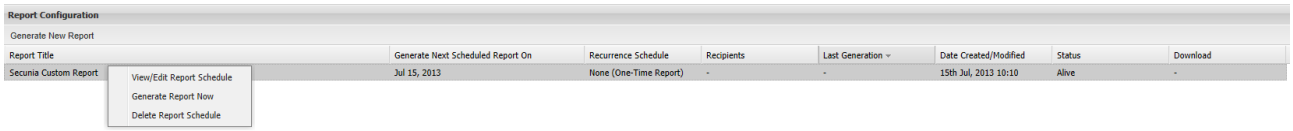



Use this page to view a list of reports that have been configured and scheduled for generation. You can configure a new report by clicking **Generate New Report** or right-click an existing report to view, edit or delete it. The Secunia CSI reporting capabilities allow the user to schedule and fully customize the intended report.

The Secunia CSI report configuration has the following options:

- **Report Generation Schedule** – Choose between a One-time only report or a recurring one (daily, weekly, monthly)
- **Executive Summary Report** – Choose to include the Executive Summary Report which provides an overall summary with the general state of vulnerability and patch management
- **Dashboard Profiles** – Choose a dashboard profile to be included in the report
- **Site Level Statistics** – Choose which sites should be included together with which statistics to include
- **Host Level Statistics** – Choose a Host Smart Group to be included together with which statistics to include
- **Product Level Statistics** – Choose a Product Smart Group to be included together with which statistics to include
- **Email Recipients** – Choose the email address of the person(s) receiving the report or, if you do not want to send the report via email, do not select any recipients
- **General Configuration Options** – Choose the name for the PDF file, set report title, and specify if you would like to include the report parameters in the report itself

Right-click a report to view, edit or delete the report schedule or generate the report.



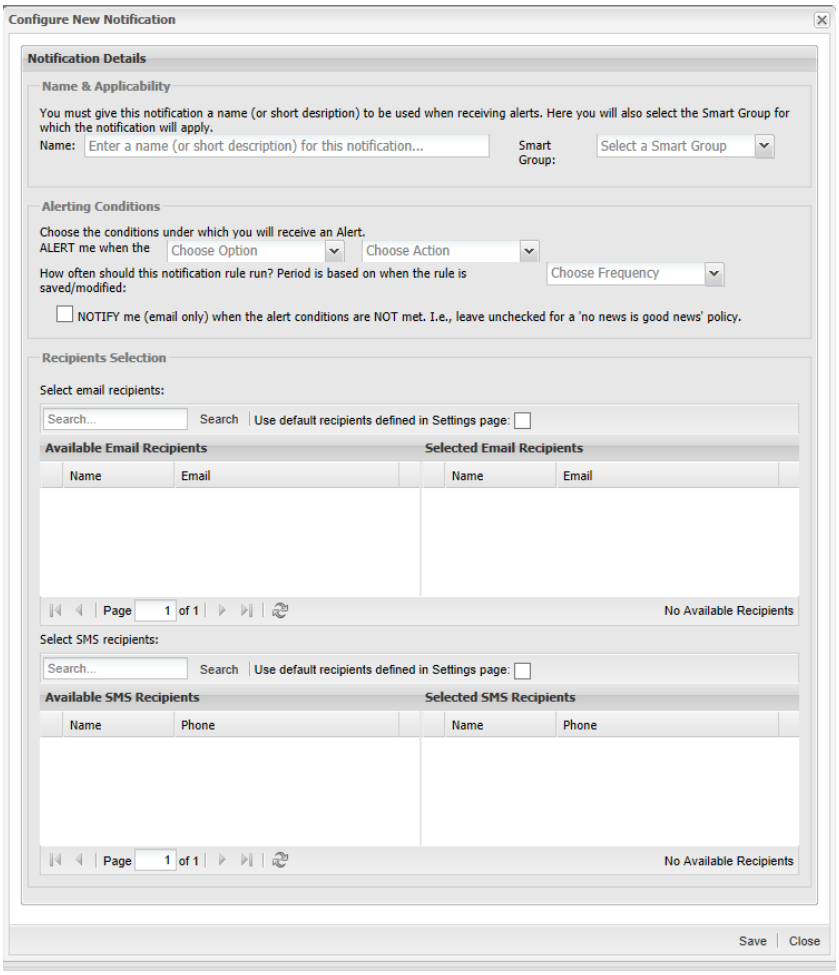

All the reports available through this feature are provided in .PDF format and will be emailed to the defined email addresses in accordance with the schedule and recurrence specified. Once generated, a report can also be downloaded directly from the main page.

The emails containing the .PDF reports will be sent from the Secunia Data Cloud - no-reply@secunia.com. Be aware that the email server from the recipient may block/filter the email if, for example, the size of the attachment exceeds a certain pre-defined threshold. If no email is being received, please check the email Spam filter and/or the Junk folder in the email client.

# Smart Group Notifications

Use this page to create and configure reminders, notifications, and alerts for a Smart Group based on the current state or changes to a group.

Click **Configure New Notification**, enter the required information and then click **Save**.

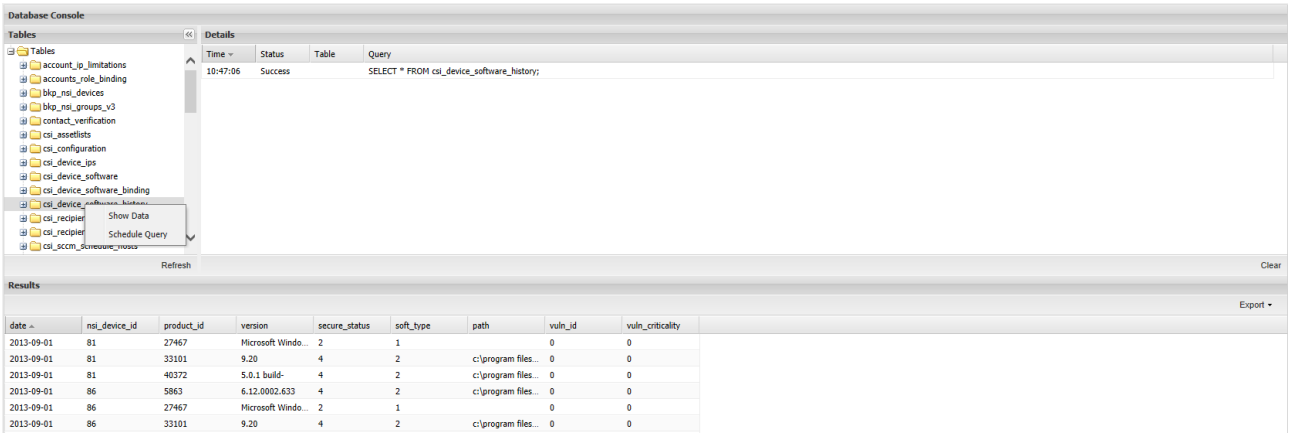

Configure New Notification
Notification Details
Name & Applicability
You must give this notification a name (or short desription) to be used when receiving alerts. Here you will also select the Smart Group for which the notification will apply.
Name:
Enter a name (or short description) for this notification...
Smart Group:
Select a Smart Group
Alerting Conditions
Choose the conditions under which you will receive an Alert.
ALERT me when the
Choose Option
Choose Action
How often should this notification rule run? Period is based on when the rule is saved/modified:
Choose Frequency
NOTIFY me (email only) when the alert conditions are NOT met. I.e., leave unchecked for a 'no news is good news' policy.
Recipients Selection
Select email recipients:
Search...
Search
Use default recipients defined in Settings page:
Available Email Recipients
Selected Email Recipients
Name
Email
Page 1 of 1
No Available Recipients
Select SMS recipients:
Search...
Search
Use default recipients defined in Settings page:
Available SMS Recipients
Selected SMS Recipients
Name
Phone
Page 1 of 1
No Available Recipients
Save
Close

Right-click a Notification in the grid to view, edit or delete it.

# Database Access

## Database Console

Use this page to access Secunia's SQL database. You can access the content of each table by selecting the table name in the **Tables** pane. Expand the table name to view the objects and data types within that table.




To create an SQL query, right-click a table and select **Show Data** to automatically create a **SELECT * FROM** table query from the specific table. You can also right-click a table and select **Schedule Query** to create a scheduled export for the table and save the output to a CSV file.

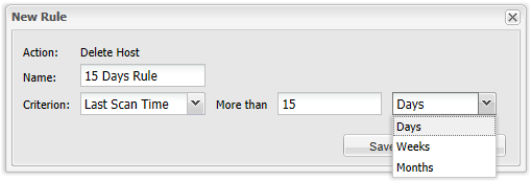
The **Details** and **Results** panes display the status of the query.

## Database Cleanup

Use this page to delete hosts from your Secunia CSI account by configuring rules that check for certain criteria.

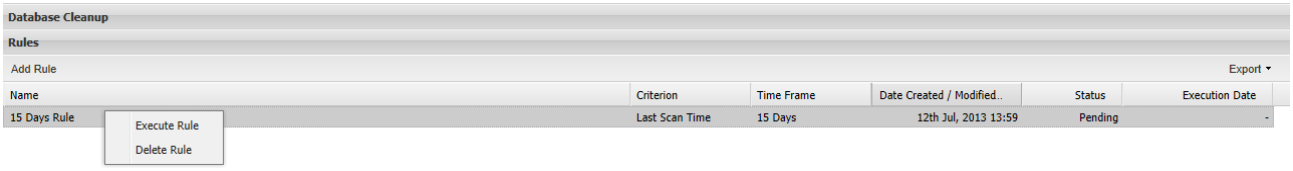
You can use this page, for example, to delete all the hosts that have not been scanned for more than 15 days.

Click **Add Rule**, enter the required information and click **Save**.




The rules can be based on **Last Scan** activity, **Last Check-in** activity or for Host that have been **Never Scanned**. Once a rule has been configured you can see which hosts meet the criteria defined in the rule and will be deleted from your Secunia CSI account.

Once you have checked the hosts to be deleted you can choose to run the rule. Right-click the rule name and select **Execute Rule**.



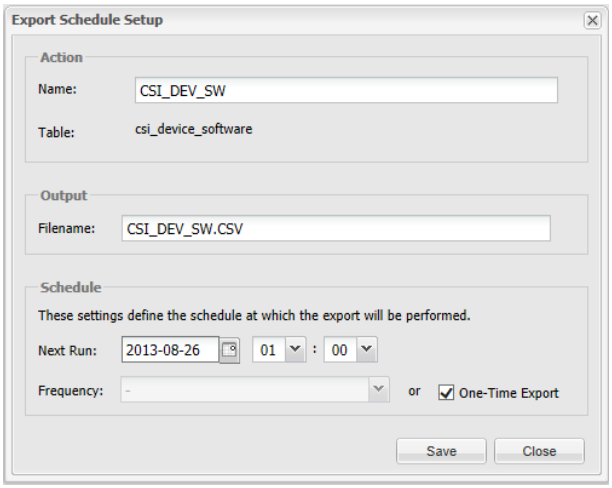
# Scheduled Exports

Use this page to view, edit or delete automated data extraction schedules.

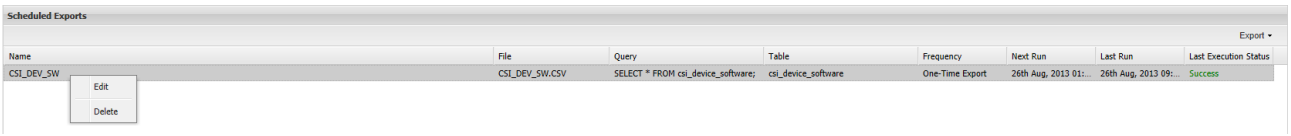
> ⚠ To schedule exports you must first download and install the Secunia Daemon. You can download the Secunia Daemon from http://secunia.com/downloadcsi/.

In the Export Schedule Setup screen, enter:

- The **Name** of the scheduled export
- The **Filename** that you want to save the CSV file as
- The **Next Run** date and time
- The **Frequency** (Hourly, Daily, Weekly or Monthly) that the export will be performed or select the **One-Time Export** check box

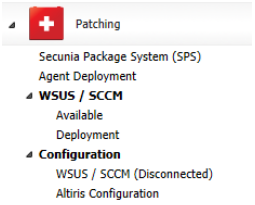



Right-click a Scheduled Export in the grid to edit or delete the export.



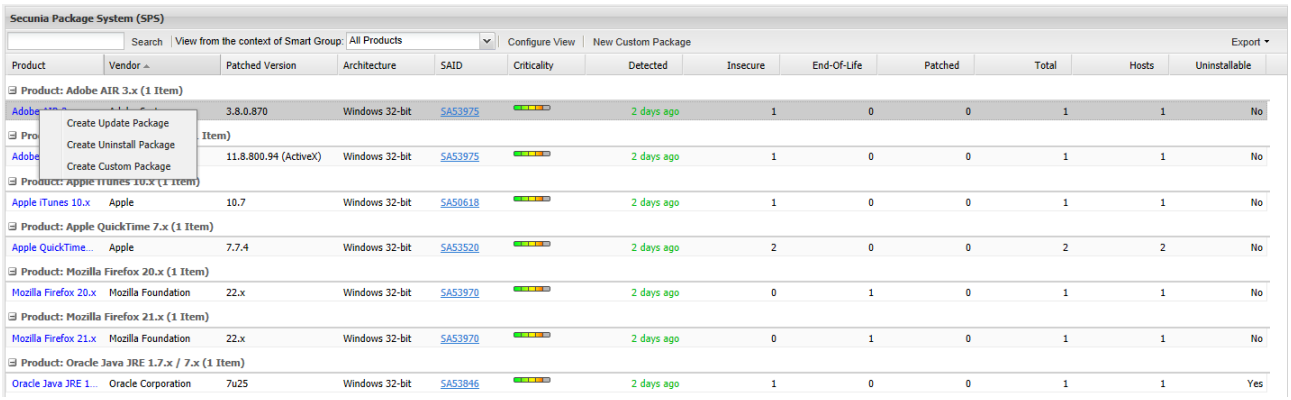
# Patching

## Secunia Package System (SPS)



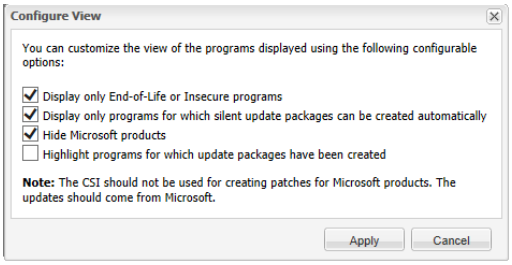

The Secunia Package System (SPS) gives administrators the ability to create packages that are capable of doing a wide range of actions; everything from updating and uninstalling third-party applications to handling complex execution flows with multiple files.

The Secunia Package System (SPS) page displays a list of products for which the Secunia CSI can automatically create an Update/Uninstall package. Right-click any of the listed products to view the available options.



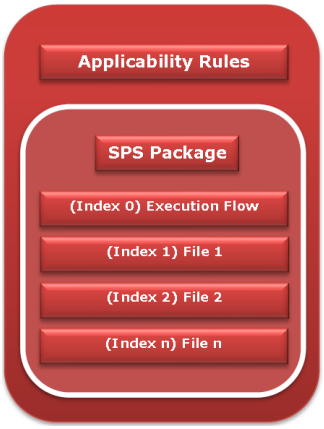

You can also target specific languages and approve packages before they are published. The package configuration, based on the product family, is retained for future use.

Click **Configure View** to select the criteria that will be used to display the products in this view.


Configure View
You can customize the view of the programs displayed using the following configurable options:
Display only End-of-Life or Insecure programs
Display only programs for which silent update packages can be created automatically
Hide Microsoft products
Highlight programs for which update packages have been created
Note: The CSI should not be used for creating patches for Microsoft products. The updates should come from Microsoft.
Apply
Cancel

# SPS Concepts and Terminology

The Secunia CSI user should become familiar with the concepts and terminology described in this section.




## What does a SPS package consists of?

The package consists of two parts; applicability rules and SPS package. The applicability rules are used by WSUS to only execute the package on computers that are applicable for the selected package.

The SPS package consists of the payload that is then executed on the computer.

The image on the right hand side illustrates the conceptual structure of a SPS package. The following sections will explain in greater detail all the components that make a SPS package.

## Applicability Rules

The applicability rules are rules used to decide whether or not a package should be offered to a client. These rules are as follows:

- **IsInstallableApplicabilityRule** – Obtains the rules for determining whether or not this item is installable on a given computer. It generally consists of paths and version information of relevant files.
- **IsInstalledApplicabilityRule** – Obtains the rules for determining whether or not this item is already installed on a given computer. It generally consists of keys and value information of relevant registry keys.
- **IsSupersededApplicabilityRule** – Obtains or sets the rules for determining whether or not this item is superseded by another update on a given computer. It generally consists of paths and version information of relevant files.

## SPS Package

The SPS package must always consist of at least one file that is placed at index "0", this is the execution flow script, and any additional files will be numbered accordingly in ascending order. The execution flow script is either JScript (JavaScript), VBScript or Powershell script; by default a JavaScript example is provided in the SPS Package Creation Wizard.

The script will be automatically extracted from the SPS package and executed. Based on the execution flow more files can then be extracted and executed from the SPS package, referenced by their index order.

## Execution Flow Script

This execution flow script is always executed. This is the file with index 0, and as such it will always be the first to run.

In the execution flow script you can define any other files to be extracted and executed. The default execution flow template that is provided in the SPS Package Creation Wizard will extract the first file supplied in the package with the specified silent parameters (usually this is the patch file provided by the vendor). Any other files added to the package will **NOT** be extracted or executed when using the example script.

If you create your own execution flow, no user interaction is available. To make your execution flow totally unattended, use log files accordingly for easy troubleshooting.

## Files

The SPS package supports additional files besides the execution flow script. The added files will have array indices from 1 to n where the first file will have index 1, and the additional files are numbered in ascending order.

# Creating a Patch with the Secunia Package System (SPS)

The Secunia Package System (SPS) page displays a list of products that you can create updates for.

Click **Configure View** to customize the list and limit the types of products shown, as well as highlight products for which packages have or have not been created.

If highlighted, products for which SPS packages exist will be shown in green.

A product will be displayed in blue if the vendor provides unattended/silent installation parameters for its patches. Any product listed in blue is available to have an update created in a simple 3 step process.

Some products are presented in grey because the vendor of the product does not provide silent installation parameters. If you choose to patch one these products, you must provide (import) the **.MSI/.MSP/.EXE** file together with the parameters for the unattended installation. The Secunia CSI will then repackage and publish the update through the standard workflow. Packages cannot be automatically created by the Secunia CSI for these products.

If you wish to create a new custom package that does not necessarily patch an existing product, for example to deploy new software, you can click **New Custom Package**. In this case you should provide the files/installer that will be executed on the target client together with the execution flow script.

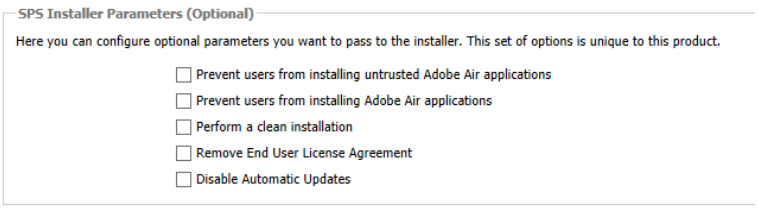
With the Secunia CSI 7.0 you are able to create three different kinds of packages. Right-click a product and select one of the available options:

- Create Update Package
- Create Uninstall Package
- Create Custom Package

For the Update and Uninstall packages a default execution flow script is provided in the SPS Package Creation Wizard (Step 2), which will fulfill most of the common needs.

The execution flow script for an Update package can also be customized for additional functionality. You can also configure your patching package SPS Installer Parameters using dynamic check box options (where applicable) based on product functionality, including:

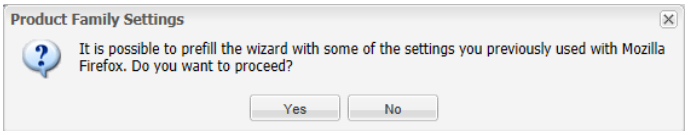
- Remove Desktop Shortcut
- Remove End User License Agreement
- Disable Automatic Updates
- Silent Install
- Update to lowest secure version
- No reboot necessary
- Cumulative updates in one package
- Set Security Level
- Remove system tray icon
- Restrict Java Applications
- Uninstall Prior to Installing
- Prevent Installation of Certain Components
- Prevent Collection of Anonymous Usage Statistics


SPS Installer Parameters (Optional)
Here you can configure optional parameters you want to pass to the installer. This set of options is unique to this product.
Prevent users from installing untrusted Adobe Air applications
Prevent users from installing Adobe Air applications
Perform a clean installation
Remove End User License Agreement
Disable Automatic Updates

# Create an Update Package

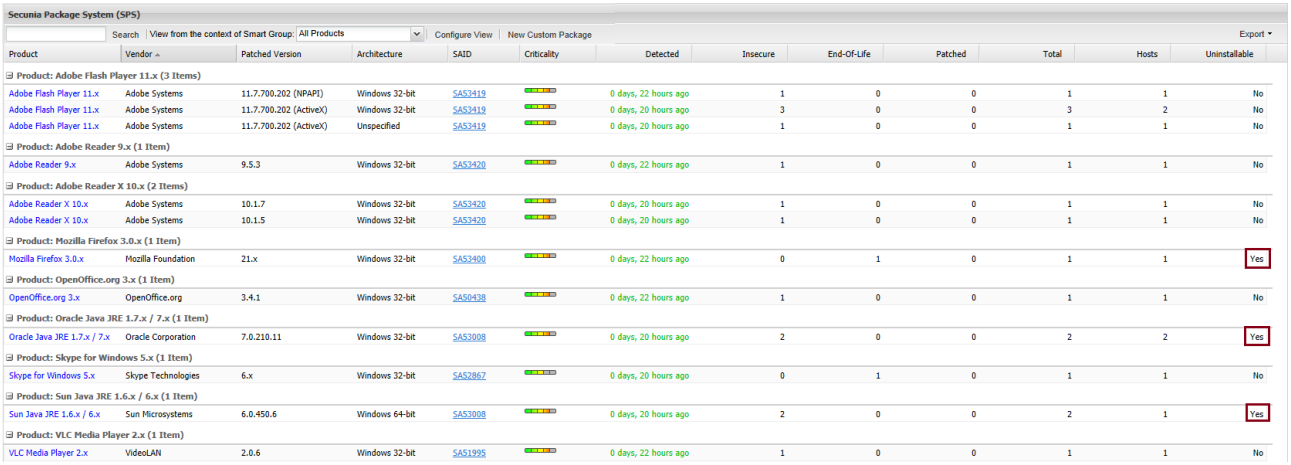
A Product will be displayed in blue if the vendor provides unattended/silent installation parameters for its patches. Any Product listed in blue is available to have an update created in a 3 step process. Right-click or double-click one of these Products and select **Create Update Package** to start the SPS Package Creation Wizard.

The Secunia CSI 7 retains Product Family Settings that you previously used. Click **Yes** to prefill the SPS Package Creation Wizard with the available settings.


Product Family Settings
It is possible to prefill the wizard with some of the settings you previously used with Mozilla Firefox. Do you want to proceed?
Yes
No

# Create an Uninstall Package

Any Products that are listed as **Yes** in the **Uninstallable** column are available to have an uninstall package created in a 3 step process exactly as the update packages in blue.


Secunia Package System (SPS)
Search
View from the context of Smart Group: All Products
Configure View
New Custom Package
Export
Product
Vendor
Patched Version
Architecture
SAID
Criticality
Detected
Insecure
End-Of-Life
Patched
Total
Hosts
Uninstallable
Product: Adobe Flash Player 11.x (3 Items)
Adobe Flash Player 11.x Adobe Systems 11.7.700.202 (NPAPI) Windows 32-bit SA53419 0 days, 22 hours ago 1 0 0 1 1 No
Adobe Flash Player 11.x Adobe Systems 11.7.700.202 (ActiveX) Windows 32-bit SA53419 0 days, 20 hours ago 3 0 0 3 2 No
Adobe Flash Player 11.x Adobe Systems 11.7.700.202 (ActiveX) Unspecified SA53419 0 days, 20 hours ago 1 0 0 1 1 No
Product: Adobe Reader 9.x (1 Item)
Adobe Reader 9.x Adobe Systems 9.5.3 Windows 32-bit SA53420 0 days, 22 hours ago 1 0 0 1 1 No
Product: Adobe Reader X 10.x (2 Items)
Adobe Reader X 10.x Adobe Systems 10.1.7 Windows 32-bit SA53420 0 days, 20 hours ago 1 0 0 1 1 No
Adobe Reader X 10.x Adobe Systems 10.1.5 Windows 32-bit SA53420 0 days, 20 hours ago 1 0 0 1 1 No
Product: Mozilla Firefox 3.0.x (1 Item)
Mozilla Firefox 3.0.x Mozilla Foundation 21.x Windows 32-bit SA53400 0 days, 22 hours ago 0 1 0 1 1 Yes
Product: OpenOffice.org 3.x (1 Item)
OpenOffice.org 3.x OpenOffice.org 3.4.1 Windows 32-bit SA50438 0 days, 22 hours ago 1 0 0 1 1 No
Product: Oracle Java JRE 1.7.x / 7.x (1 Item)
Oracle Java JRE 1.7.x / 7.x Oracle Corporation 7.0.210.11 Windows 32-bit SA53008 0 days, 20 hours ago 2 0 0 2 2 Yes
Product: Skype for Windows 5.x (1 Item)
Skype for Windows 5.x Skype Technologies 6.x Windows 32-bit SA52867 0 days, 20 hours ago 0 1 0 1 1 No
Product: Sun Java JRE 1.6.x / 6.x (1 Item)
Sun Java JRE 1.6.x / 6.x Sun Microsystems 6.0.450.6 Windows 64-bit SA53008 0 days, 20 hours ago 2 0 0 2 1 Yes
Product: VLC Media Player 2.x (1 Item)
VLC Media Player 2.x VideoLAN 2.0.6 Windows 32-bit SA51995 0 days, 22 hours ago 1 0 0 1 1 No

For Products listed as **No** in the **Uninstallable** column you must customize the execution flow script to successfully uninstall the product. This can be done by starting the SPS Package Creation Wizard and selecting the **Edit Package Content** check box in Step 1.

If you have an SPS XML template you can import it by clicking **Import Package** in the first step of the wizard. Once this is completed, all the fields in the wizard will be automatically populated, including the execution flow script.

Special attention should be given to the files mentioned in the execution flow script. These files can be files originally provided by the SPS template creator or they can be dynamically downloaded.

> ⚠ You should only import SPS packages if you trust the author of the package and the source from where you downloaded/obtained the package.

## Create a Custom Package

The Secunia CSI 7.0 allows creating custom packages that can be deployed through WSUS/System Center Configuration Manager. By creating a custom package you can do a wide range of actions; everything from updating and uninstalling third-party applications to handling complex execution flows with multiple files.

The creation of a custom package can be done in two different ways. Either:

- Right-click a product and choose **Create Custom Package**. By doing this the product applicability rules will be included in the package; this will mean that the Custom Package will only be applicable for computers with the selected product installed.

  OR

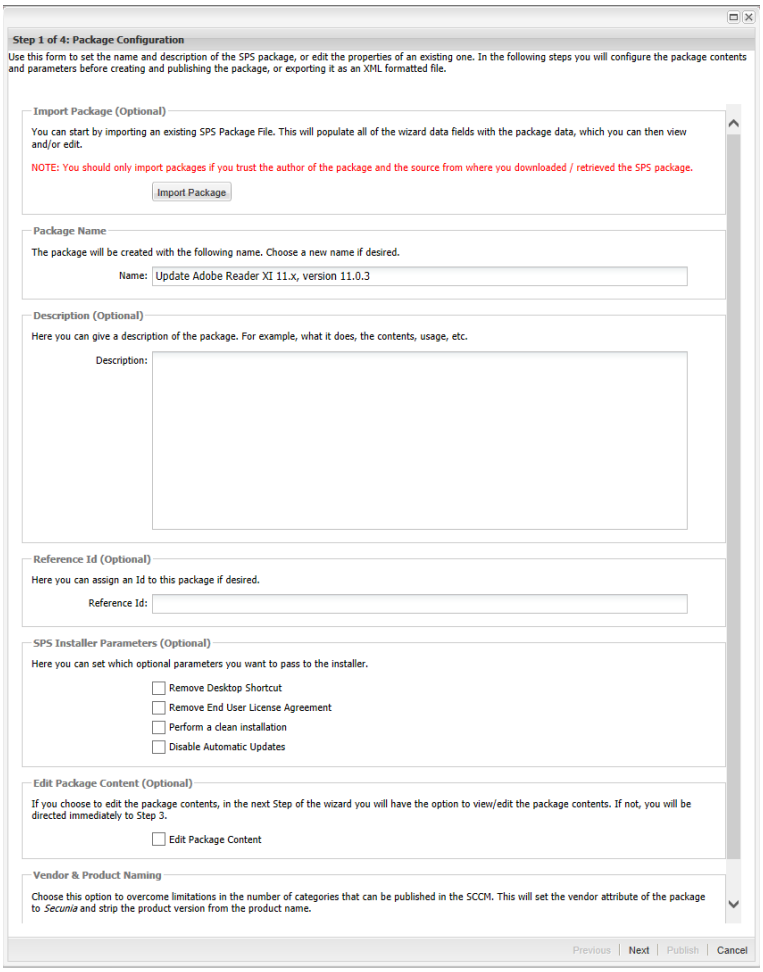
- Click **New Custom Package** to start the SPS Package Creation Wizard. In this case no applicability rules will limit the installation base.

Independently of the chosen approach, in both cases the SPS Package Creation Wizard will be initiated.

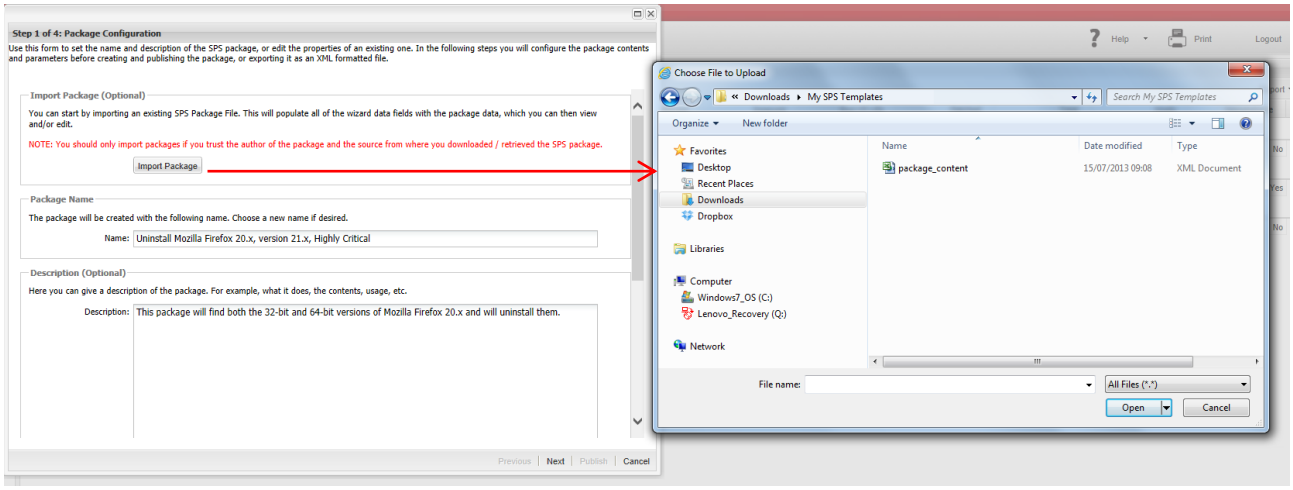
# The SPS Package Creation Wizard

## Step 1 of 4: Package Configuration

In Step 1 no action is required if the selected product was in blue. You should only check **Edit Package Content (Optional)** if the product was in grey or there is a need to customize the update patch by selecting a different file(s) and/or defining a different execution flow script.


Step 1 of 4: Package Configuration
Use this form to set the name and description of the SPS package, or edit the properties of an existing one. In the following steps you will configure the package contents and parameters before creating and publishing the package, or exporting it as an XML formatted file.
Import Package (Optional)
You can start by importing an existing SPS Package File. This will populate all of the wizard data fields with the package data, which you can then view and/or edit.
NOTE: You should only import packages if you trust the author of the package and the source from where you downloaded / retrieved the SPS package.
Import Package
Package Name
The package will be created with the following name. Choose a new name if desired.
Name:
Update Adobe Reader XI 11.x, version 11.0.3
Description (Optional)
Here you can give a description of the package. For example, what it does, the contents, usage, etc.
Description:
Reference Id (Optional)
Here you can assign an Id to this package if desired.
Reference Id:
SPS Installer Parameters (Optional)
Here you can set which optional parameters you want to pass to the installer.
Remove Desktop Shortcut
Remove End User License Agreement
Perform a clean installation
Disable Automatic Updates
Edit Package Content (Optional)
If you choose to edit the package contents, in the next Step of the wizard you will have the option to view/edit the package contents. If not, you will be directed immediately to Step 3.
Edit Package Content
Vendor & Product Naming
Choose this option to overcome limitations in the number of categories that can be published in the SCCM. This will set the vendor attribute of the package to Secunia and strip the product version from the product name.
Previous
Next
Publish
Cancel

The **Import Package** feature allows you to import a SPS template in XML format that will automatically populate all the fields of the SPS Package Creation Wizard. This feature will be especially relevant when creating custom updates or when creating update packages for the products in grey.

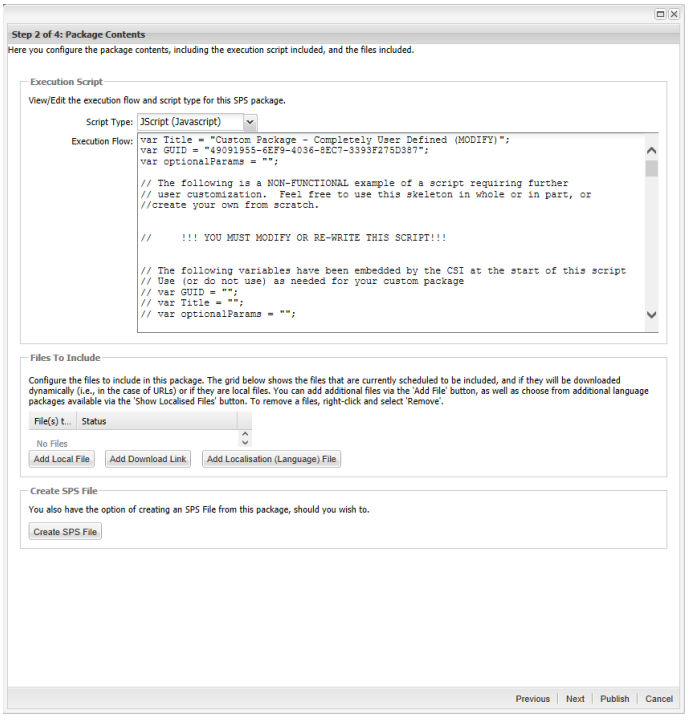

Step 1 of 4: Package Configuration
Use this form to set the name and description of the SPS package, or edit the properties of an existing one. In the following steps you will configure the package contents and parameters before creating and publishing the package, or exporting it as an XML formatted file.
Import Package (Optional)
You can start by importing an existing SPS Package File. This will populate all of the wizard data fields with the package data, which you can then view and/or edit.
NOTE: You should only import packages if you trust the author of the package and the source from where you downloaded / retrieved the SPS package.
Import Package
Package Name
The package will be created with the following name. Choose a new name if desired.
Name: Uninstall Mozilla Firefox 20.x, version 21.x, Highly Critical
Description (Optional)
Here you can give a description of the package. For example, what it does, the contents, usage, etc.
Description: This package will find both the 32-bit and 64-bit versions of Mozilla Firefox 20.x and will uninstall them.
Previous
Next
Publish
Cancel
Help
Print
Logout
Choose File to Upload
Downloads
My SPS Templates
Search My SPS Templates
Organize
New folder
Favorites
Desktop
Recent Places
Downloads
Dropbox
Libraries
Computer
Windows7_OS (C:)
Lenovo_Recovery (Q:)
Network
Name
Date modified
Type
package_content
15/07/2013 09:08
XML Document
File name:
All Files (*.*)
Open
Cancel

In Step 4 of the wizard you will also have the option to export the XML template for the package being created.

After clicking **Next**, and if **Edit Package Content (Optional)** was not selected, you will go directly to Step 3 of 4: Applicability Criteria - Paths.

## Step 2 of 4: Package Contents

Step 2 becomes available when **Edit Package Content** is selected in Step 1. The first section of Step 2 is the Execution Script where you select **JScript (Javascript)**, **VBScript** or **Powershell Script** and then review or create a customized execution flow.


Step 2 of 4: Package Contents
Here you configure the package contents, including the execution script included, and the files included.
Execution Script
View/Edit the execution flow and script type for this SPS package.
Script Type: JScript (Javascript)
Execution Flow:
var Title = "Custom Package - Completely User Defined (MODIFY)";
var GUID = "49091955-6EF9-4036-8EC7-3393F275D387";
var optionalParams = "";
// The following is a NON-FUNCTIONAL example of a script requiring further
// user customization. Feel free to use this skeleton in whole or in part, or
//create your own from scratch.
// !!! YOU MUST MODIFY OR RE-WRITE THIS SCRIPT!!!
// The following variables have been embedded by the CSI at the start of this script
// Use (or do not use) as needed for your custom package
// var GUID = "";
// var Title = "";
// var optionalParams = "";
Files To Include
Configure the files to include in this package. The grid below shows the files that are currently scheduled to be included, and if they will be downloaded dynamically (i.e., in the case of URLs) or if they are local files. You can add additional files via the 'Add File' button, as well as choose from additional language packages available via the 'Show Localised Files' button. To remove a files, right-click and select 'Remove'.
File(s) t...
Status
No Files
Add Local File
Add Download Link
Add Localisation (Language) File
Create SPS File
You also have the option of creating an SPS File from this package, should you wish to.
Create SPS File
Previous
Next
Publish
Cancel

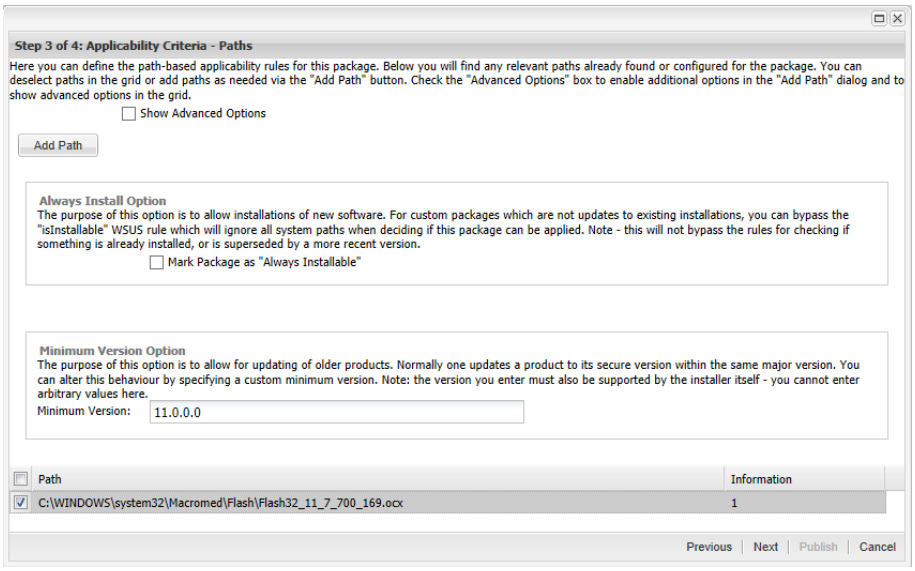
You are also able to change the files that are included in the SPS package, which can either be local files or links to be dynamically downloaded upon publishing of the package.

To test a newly created execution flow together with the added files click **Create SPS File**. A SPS.exe file is created that can be executed locally prior to being published into the WSUS server.

This SPS.exe file will include the execution flow script and the files to be included, but not the applicability rules.

## Step 3 of 4: Applicability Criteria - Paths

In Step 3 you should select the paths/locations to which this package should be applied. These are usually populated by the Secunia CSI based on the scans previously conducted.


Step 3 of 4: Applicability Criteria - Paths
Here you can define the path-based applicability rules for this package. Below you will find any relevant paths already found or configured for the package. You can deselect paths in the grid or add paths as needed via the "Add Path" button. Check the "Advanced Options" box to enable additional options in the "Add Path" dialog and to show advanced options in the grid.
Show Advanced Options
Add Path
Always Install Option
The purpose of this option is to allow installations of new software. For custom packages which are not updates to existing installations, you can bypass the "isInstallable" WSUS rule which will ignore all system paths when deciding if this package can be applied. Note - this will not bypass the rules for checking if something is already installed, or is superseded by a more recent version.
Mark Package as "Always Installable"
Minimum Version Option
The purpose of this option is to allow for updating of older products. Normally one updates a product to its secure version within the same major version. You can alter this behaviour by specifying a custom minimum version. Note: the version you enter must also be supported by the installer itself - you cannot enter arbitrary values here.
Minimum Version:
11.0.0.0
Path
Information
C:\WINDOWS\system32\Macromed\Flash\Flash32_11_7_700_169.ocx
1
Previous
Next
Publish
Cancel

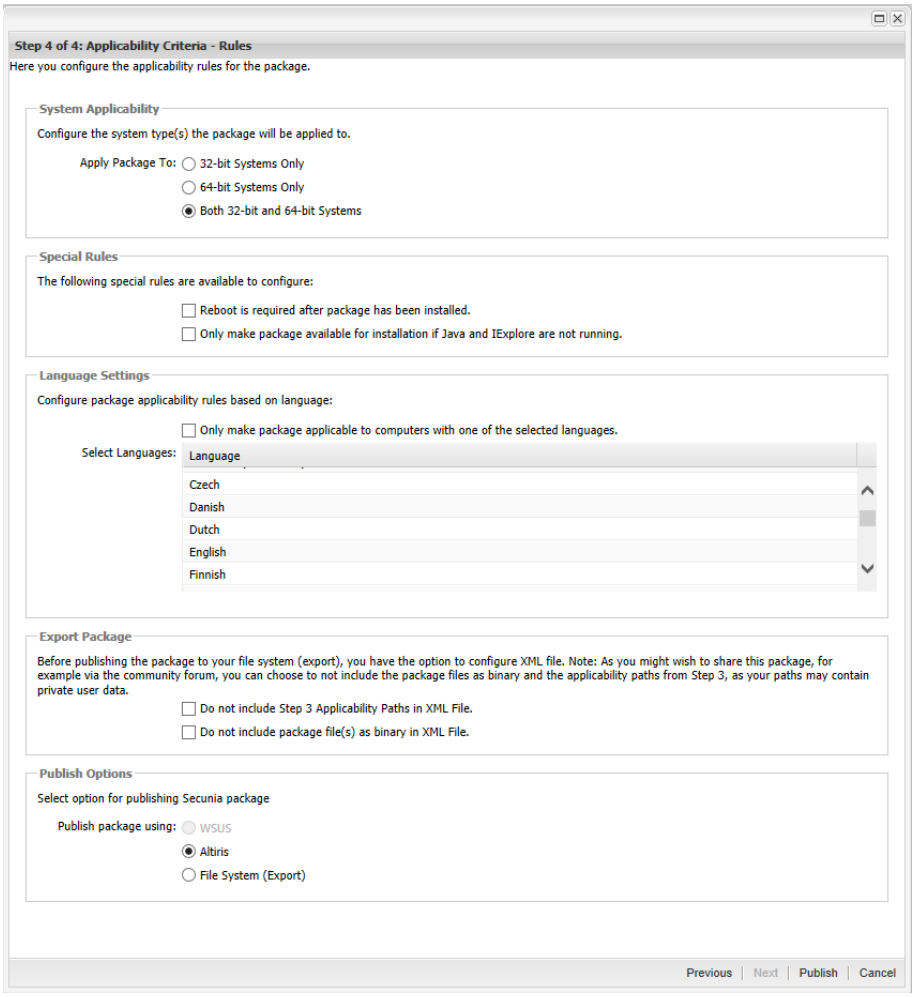
Please be advised to only choose paths that are valid to avoid any update loops. You can also use paths with CSIDL and KNOWNFOLDERID (http://msdn.microsoft.com/en-us/library/bb762494%28v=vs.85%29.aspx) if you select the **Show Advanced Options** check box. These variables should be used with their decimal value.

For packages that should not have any paths for applicability, select the **Mark Package as "Always Installable"** check box to ignore all paths. Paths for App-V and Mac OS X are filtered out since they are not supported for patching.

Use the **Minimum Version Option** to update older products. Normally, a product is updated to its secure version within the same major version. You can alter this behavior by specifying a custom minimum version. Note: the version you enter must also be supported by the installer itself - you cannot enter arbitrary values here.

# Step 4 of 4: Applicability Criteria - Rules

In Step 4 you should specify if you want to limit the package to 32-bit or 64-bit systems or computers with specific operating system languages. The patch file to be deployed will be automatically downloaded in the background by the Secunia CSI console. Once this is completed the Secunia CSI console will repackage and publish the update package into the WSUS/System Center Configuration Manager.


Step 4 of 4: Applicability Criteria - Rules
Here you configure the applicability rules for the package.
System Applicability
Configure the system type(s) the package will be applied to.
Apply Package To:
32-bit Systems Only
64-bit Systems Only
Both 32-bit and 64-bit Systems
Special Rules
The following special rules are available to configure:
Reboot is required after package has been installed.
Only make package available for installation if Java and IExplore are not running.
Language Settings
Configure package applicability rules based on language:
Only make package applicable to computers with one of the selected languages.
Select Languages:
Language
Czech
Danish
Dutch
English
Finnish
Export Package
Before publishing the package to your file system (export), you have the option to configure XML file. Note: As you might wish to share this package, for example via the community forum, you can choose to not include the package files as binary and the applicability paths from Step 3, as your paths may contain private user data.
Do not include Step 3 Applicability Paths in XML File.
Do not include package file(s) as binary in XML File.
Publish Options
Select option for publishing Secunia package
Publish package using:
WSUS
Altiris
File System (Export)
Previous
Next
Publish
Cancel

The WSUS option will be unavailable if the WSUS Connection is not established.

To export the package select **File System (Export)** and click **Publish**.

If a reboot is required after the package has been installed this can also be configured in the second part of this step as well as checking if java is running.

To configure your package to only be applicable for certain languages of the operating system, select **Only make package applicable to computers with one of the selected languages** and select the relevant language.

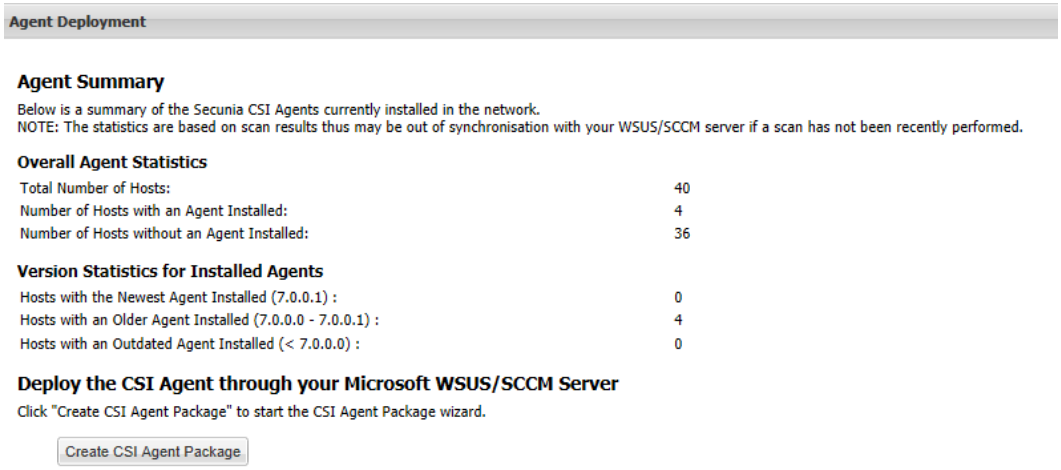
In this step you are also able to export the package that you have already configured to be used for future reference. You have the option to include or exclude Step 3 applicability paths and the installer as binary.

The two options (**Do not include Step 3 Applicability Paths in XML File** and **Do not include the package file(s) as binary in XML File**) are taken into consideration only when exporting the package to the **File System (Export)**, otherwise the selection will be disregarded.

# Agent Deployment

If you choose to scan the target host by using the Secunia CSI Agent in Single Host mode (recommended), you can easily distribute and install the Agent by deploying it through WSUS/System Center Configuration Manager.

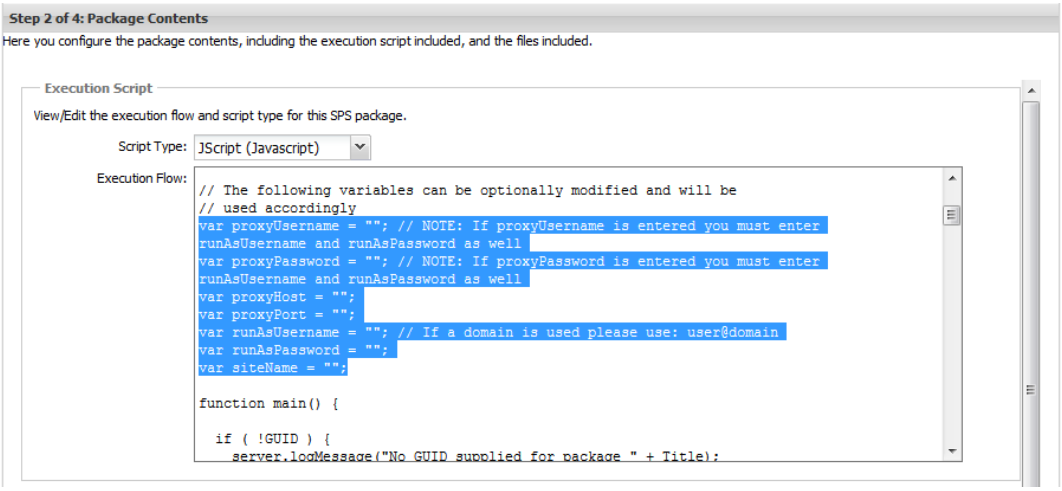
Click **Create CSI Agent Package** under **Agent Deployment** to start the CSI Agent Package wizard.


Agent Deployment
Agent Summary
Below is a summary of the Secunia CSI Agents currently installed in the network.
NOTE: The statistics are based on scan results thus may be out of synchronisation with your WSUS/SCCM server if a scan has not been recently performed.
Overall Agent Statistics
Total Number of Hosts: 40
Number of Hosts with an Agent Installed: 4
Number of Hosts without an Agent Installed: 36
Version Statistics for Installed Agents
Hosts with the Newest Agent Installed (7.0.0.1) : 0
Hosts with an Older Agent Installed (7.0.0.0 - 7.0.0.1) : 4
Hosts with an Outdated Agent Installed (< 7.0.0.0) : 0
Deploy the CSI Agent through your Microsoft WSUS/SCCM Server
Click "Create CSI Agent Package" to start the CSI Agent Package wizard.
Create CSI Agent Package

The CSI Agent Package can be created and managed just like any other Secunia SPS package.

# Add Proxy Settings

You can add proxy settings to the installation script in the SPS wizard when creating the agent deployment package. In **Step 2 of 4: Package Contents**, modify the variables in the Execution Flow field:

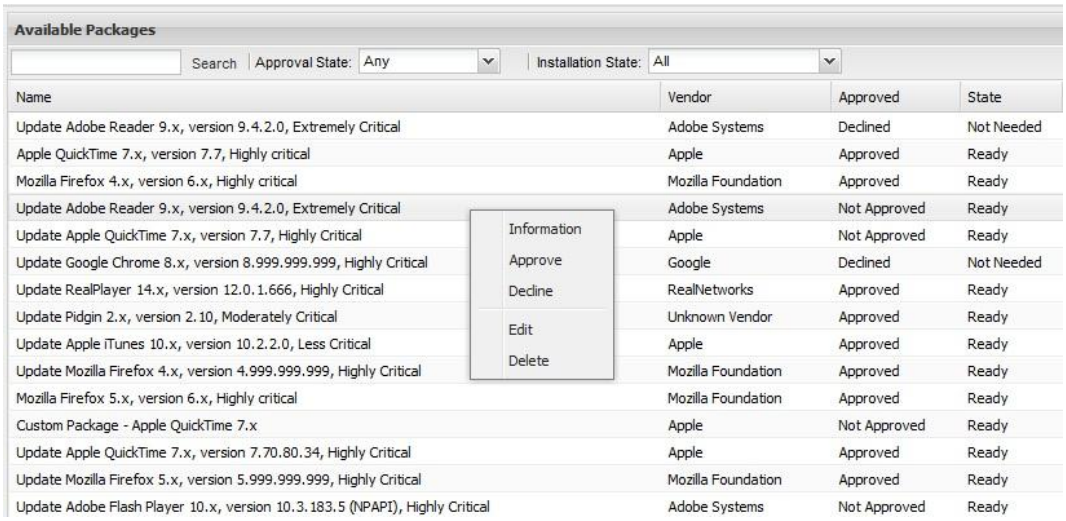

Step 2 of 4: Package Contents
Here you configure the package contents, including the execution script included, and the files included.
Execution Script
View/Edit the execution flow and script type for this SPS package.
Script Type: JScript (Javascript)
Execution Flow:
// The following variables can be optionally modified and will be
// used accordingly
var proxyUsername = ""; // NOTE: If proxyUsername is entered you must enter
runAsUsername and runAsPassword as well
var proxyPassword = ""; // NOTE: If proxyPassword is entered you must enter
runAsUsername and runAsPassword as well
var proxyHost = "";
var proxyPort = "";
var runAsUsername = ""; // If a domain is used please use: user@domain
var runAsPassword = "";
var siteName = "";
function main() {
if ( !GUID ) {
server.logMessage("No GUID supplied for package " + Title);

# WSUS/System Center Configuration Manager

## Available

Use this page to view a list of all the created packages that are currently published into your WSUS.

Right-click a package for more options such as **Approve**, **Decline** or **Delete** or double-click a package to display additional status details.




⚠ Once the updates have been published into the WSUS, the same rules previously configured for the Microsoft updates will apply to the updates created by the Secunia CSI. If the updates automatically appear with the Approved status, this means that this setting is being inherited from the WSUS.

## Deployment

Use this page to view a host's information collected from the WSUS Server. Use the **Installation State** drop-down list to filter the hosts being displayed.

Right-click a host and select **Information** to view additional details such as: **Scan Result**, **Patch Information**, **Patches Available** and **Overview**.

You can also right-click a host listed in this view and select **Verify and Install Certificate** to install the required certificate created or imported in Step 2 – Certificate Status.

Usually the certificate is installed through a GPO as described in Step 3 – Group Policy Status.

In order to successfully install the certificate, ensure you have started the Secunia CSI console with **Domain Administrator** privileges. In Windows Vista, 7, 8 or 2008, right-click the CSI icon and select **Run as administrator**.

Also note that the Remote Registry must be enabled on hosts for which you intend to install the certificate using the Secunia CSI GUI. The remote registry is not needed if distributing the certificate through GPO.

The WSUS Self-Signed Certificate can also be installed through a manually created Group Policy.

### Deploying the Update Package Using WSUS

In order to deploy the update package using WSUS, the update package must be approved. After publishing the package into the WSUS, and assuming that the update is visible under **Available**, right-click the package name and select **Approve**.

You will be prompted to select the computer target groups for which you would like to approve the update. These target groups are configured in the WSUS.

The same approach should be used if you wish to decline a previously approved update.

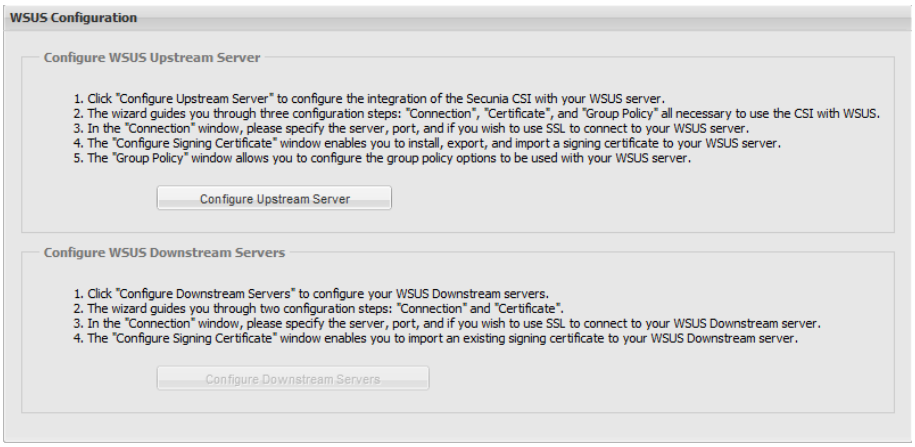
### Deploying the Update Package Using System Center Configuration Manager

The actions **Approve** and **Decline** are only applicable if the package is to be deployed through WSUS. If you are using the Microsoft System Center Configuration Manager, the package created with the Secunia CSI will be available in your System Center Configuration Manager.

# Configuration

## WSUS/System Center Configuration Manager

Use this option to configure the integration of the Secunia CSI with your WSUS server(s). If you have a single WSUS server, which is connected to Microsoft Updates site, running the **Configure Upstream Server** wizard will be sufficient for setting up the Secunia CSI with WSUS.


WSUS Configuration
Configure WSUS Upstream Server
1. Click "Configure Upstream Server" to configure the integration of the Secunia CSI with your WSUS server.
2. The wizard guides you through three configuration steps: "Connection", "Certificate", and "Group Policy" all necessary to use the CSI with WSUS.
3. In the "Connection" window, please specify the server, port, and if you wish to use SSL to connect to your WSUS server.
4. The "Configure Signing Certificate" window enables you to install, export, and import a signing certificate to your WSUS server.
5. The "Group Policy" window allows you to configure the group policy options to be used with your WSUS server.
Configure Upstream Server
Configure WSUS Downstream Servers
1. Click "Configure Downstream Servers" to configure your WSUS Downstream servers.
2. The wizard guides you through two configuration steps: "Connection" and "Certificate".
3. In the "Connection" window, please specify the server, port, and if you wish to use SSL to connect to your WSUS Downstream server.
4. The "Configure Signing Certificate" window enables you to import an existing signing certificate to your WSUS Downstream server.
Configure Downstream Servers

After clicking **Configure Upstream Server**, a configuration wizard will be initiated.

Follow the wizard steps to successfully integrate the Secunia CSI with your Microsoft WSUS.

To learn more about Microsoft WSUS please visit:

http://technet.microsoft.com/en-us/windowsserver/bb332157

The WSUS 3.0 SP2 Step By Step Guide is available at:

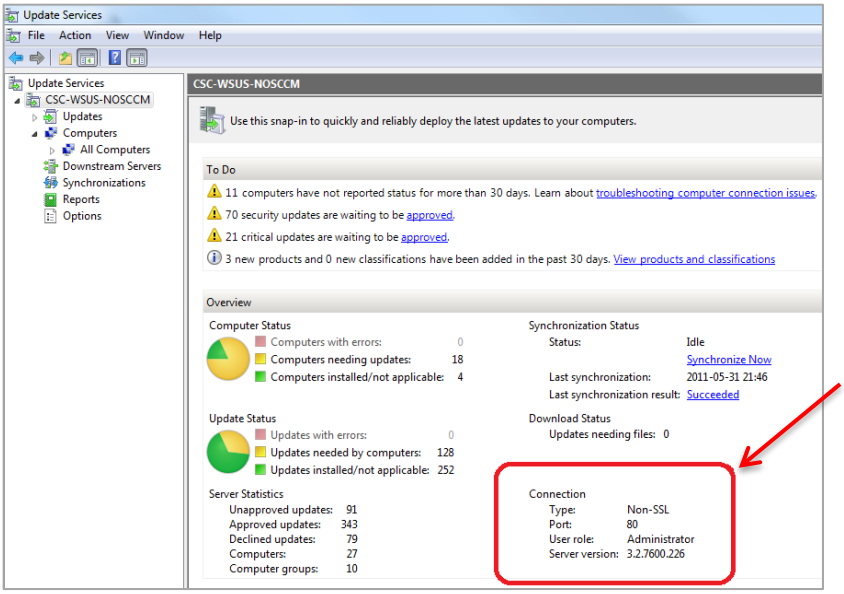
http://technet.microsoft.com/en-us/library/dd939822%28WS.10%29.aspx

The Windows Server Update Services 3.0 SP2 Technical Reference is available at:
http://technet.microsoft.com/en-us/library/hh334981%28WS.10%29.aspx

# Step 1 – Connection Status

In Step 1 you should provide the relevant information (NetBIOS name and port number) for the main Upstream WSUS server. After inserting the required information, click **Connect**.

To check the status of the connection, expand **Step 1.Connection Status**.




If you are unsure of which port number to use, check your WSUS configuration as shown.

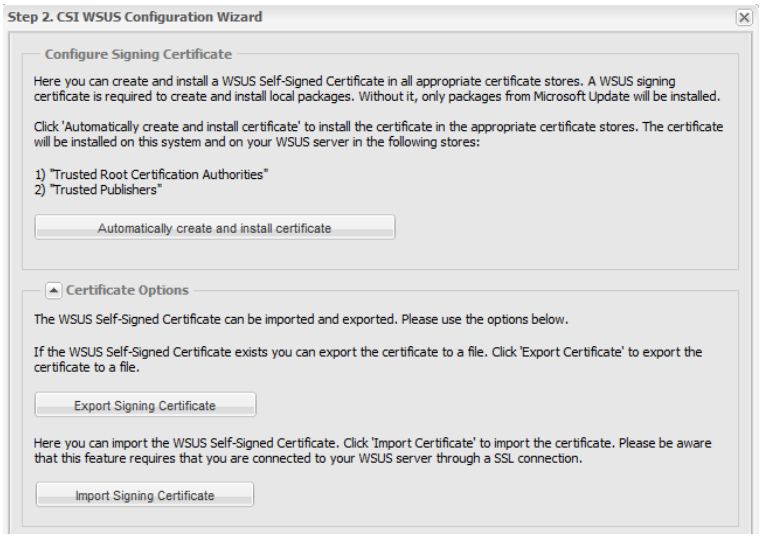
⚠ If you have a WSUS server hierarchy with one or more Downstream Replica WSUS server(s) connected to an Upstream WSUS server, please run the **Configure Downstream Servers** after running the **Configure Upstream Server** wizard.

The port number used to connect to your WSUS depends on your settings. Ports 80 or 8530 are commonly used when SSL is not configured. Only select the **Use SSL Connection** check box if your WSUS is configured to accept SSL connections.

Refer to http://technet.microsoft.com/en-us/library/bb633246.aspx for further information on how to configure WSUS to use SSL.

# Step 2 – Certificate Status

A code-signing certificate is needed to publish third-party updates to WSUS/System Center Configuration Manager so they can be deployed as patches. In this Step the Secunia CSI can request the WSUS to create and install the WSUS Self-Signed Certificate.


Step 2. CSI WSUS Configuration Wizard
Configure Signing Certificate
Here you can create and install a WSUS Self-Signed Certificate in all appropriate certificate stores. A WSUS signing certificate is required to create and install local packages. Without it, only packages from Microsoft Update will be installed.
Click 'Automatically create and install certificate' to install the certificate in the appropriate certificate stores. The certificate will be installed on this system and on your WSUS server in the following stores:
1) "Trusted Root Certification Authorities"
2) "Trusted Publishers"
Automatically create and install certificate
Certificate Options
The WSUS Self-Signed Certificate can be imported and exported. Please use the options below.
If the WSUS Self-Signed Certificate exists you can export the certificate to a file. Click 'Export Certificate' to export the certificate to a file.
Export Signing Certificate
Here you can import the WSUS Self-Signed Certificate. Click 'Import Certificate' to import the certificate. Please be aware that this feature requires that you are connected to your WSUS server through a SSL connection.
Import Signing Certificate

To create and install a WSUS Self-Signed Certificate in all appropriate certificate stores, click **Automatically create and install certificate**.

The WSUS Self-Signing Certificate must be installed/provisioned in the following systems:

- WSUS Server
- The system running CSI (note that the certificate must also be installed on the system running the CSI console)
- Clients receiving the Update

The created certificate is required and it will be used for all future publishing. Without it, only packages from Microsoft Update will be installed.

If you would like to use your own CA certificate instead of the Microsoft WSUS Self-Signing Certificate, click **Import Signing Certificate**.

At Step 3 – Group Policy Status, the certificate created/imported in this step will be provisioned to all clients through a GPO.

⚠ Be careful not to re-provision a signing certificate on a WSUS server that already has a signing certificate assigned. Doing so can cause issues with certificate validation at the WSUS server and target computers unless BOTH certificates (new and old) are left in the appropriate certificates stores (Trusted Publishers and Trusted Root Authorities). It can also cause issues with troubleshooting.

Once a certificate is either inserted or created it does not need to be re-created until it expires or needs to be replaced.

Click **Automatically create and install certificate**. The certificate will be installed on the WSUS server in the following stores:

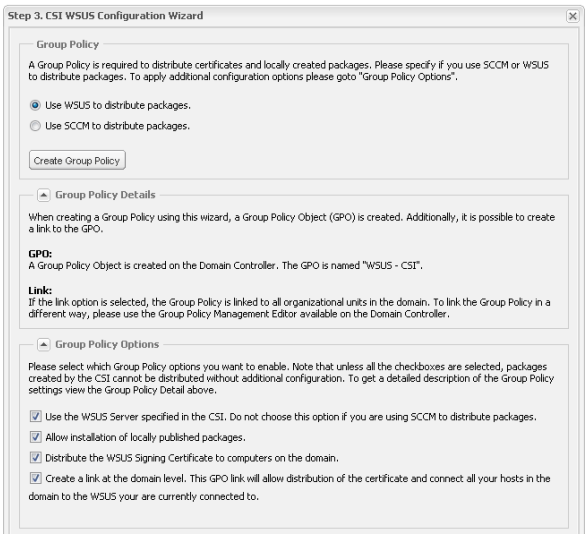
- Trusted Root Certification Authorities
- Trusted Publishers
- WSUS – The certificate in this location must also contain the private key

Expand the Certificate Options to access the import and export certificate features.

> ⚠ Be aware that in order to import your own certificate through the Secunia CSI, the WSUS connection must be configured to accept SSL connections.

## Step 3 – Group Policy Status

A Group Policy is required to distribute certificates and locally created packages. The Secunia CSI can easily create this GPO so the WSUS Signing Certificate is distributed to all clients. Please choose to use WSUS or System Center Configuration Manager. Once this is completed expand the Group Policy Options.


Step 3. CSI WSUS Configuration Wizard
Group Policy
A Group Policy is required to distribute certificates and locally created packages. Please specify if you use SCCM or WSUS to distribute packages. To apply additional configuration options please goto "Group Policy Options".
Use WSUS to distribute packages.
Use SCCM to distribute packages.
Create Group Policy
Group Policy Details
When creating a Group Policy using this wizard, a Group Policy Object (GPO) is created. Additionally, it is possible to create a link to the GPO.
GPO:
A Group Policy Object is created on the Domain Controller. The GPO is named "WSUS - CSI".
Link:
If the link option is selected, the Group Policy is linked to all organizational units in the domain. To link the Group Policy in a different way, please use the Group Policy Management Editor available on the Domain Controller.
Group Policy Options
Please select which Group Policy options you want to enable. Note that unless all the checkboxes are selected, packages created by the CSI cannot be distributed without additional configuration. To get a detailed description of the Group Policy settings view the Group Policy Detail above.
Use the WSUS Server specified in the CSI. Do not choose this option if you are using SCCM to distribute packages.
Allow installation of locally published packages.
Distribute the WSUS Signing Certificate to computers on the domain.
Create a link at the domain level. This GPO link will allow distribution of the certificate and connect all your hosts in the domain to the WSUS your are currently connected to.

If you are creating the CSI WSUS Group Policy for the first time, proceed by selecting all the options and then click **Create Group Policy**.

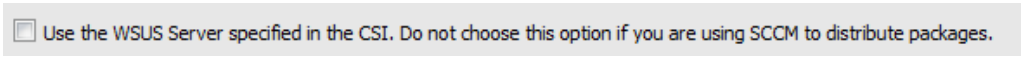
> ⚠ Besides distributing the certificate through the CSI WSUS GPO, it is also possible to provision certificate to the target computers by going to **Patching > WSUS/SCCM > Deployment**, selecting the target hosts where the certificate is to be installed (CTRL+ mouse click for multiple selection) and then right-click and select **Verify and Install Certificate**.

Remote Registry service (disabled by default on Win7/Vista) should be enabled and started for the certificate to be successfully installed.

If you prefer to create your own Group Policy to distribute the WSUS Signing Certificate, please refer to our online FAQ http://secunia.com/vulnerability_scanning/corporate/faq/.

If you prefer not to create the CSI WSUS Group Policy, the existing Windows Updates GPOs must be edited in accordance with Setting Up Clients to Access WSUS.

If you use **Microsoft System Center Configuration Manager** please make sure you do not select the first option **Use the WSUS Server specified in the CSI**.




If you already have the Windows Updates being configured through a Group Policy, we suggest you select the first 3 options in the **Create a new CSI WSUS Group Policy** page.

The CSI WSUS Group Policy will be created but not linked to your domain. This way you can easily check the details of the newly created GPO and verify that the existing WSUS GPOs are correctly configured.

## Setting Up Clients to Access WSUS

The Secunia CSI 7.0 uses the WSUS/System Center Configuration Manager to deploy patches to third-party software by leveraging the existing Microsoft deployment mechanism.

If you are not using WSUS to deploy Microsoft updates in your network you must configure your clients to check for updates against the WSUS.

The connection between the Secunia CSI and the WSUS/System Center Configuration Manager server is done with a help of a wizard. In Step 3 of the wizard you can create a Group Policy that will enable your clients to receive updates from the WSUS server.

If you choose not to create a new Group Policy using the CSI WSUS Group Policy wizard, please edit your existing WSUS Group Policy as follows:

1. In the Group Policy Management Console (GPMC), browse to the Group Policy Object (GPO) on which you want to configure WSUS and click **Edit**.
2. In the GPMC, expand **Computer Configuration**, expand **Administrative Templates**, expand **Windows Components**, and click **Windows Update**. Select:
   - ✓ **Enable:** Configure Automatic Updates (choose your settings)
   - ✓ **Enable:** Specify intranet Microsoft update service location (add the hostname/IP of your WSUS server)
   - ✓ **Enable:** Allow signed updates from an intranet Microsoft update service location (**Important** – enables WSUS to distribute patches through the Secunia CSI)

For installing the WSUS server in your environment we recommend reading the **Step by Step Installation Guide** provided by Microsoft:
http://technet.microsoft.com/en-us/wsus/default.aspx

## Third-Party Integration

The Secunia CSI 7.0 provides you with the capability of publishing packages using third-party patch deployment solutions, for example Altiris. In order to support this feature Secunia has enhanced the package export feature. The exported xml file contains additional information that can be helpful in creating packages in other tools, including:

- The version numbers
- The executable itself
- The vulnerability/criticality

Secunia has retained the simplicity of the xml file by giving you the options to exclude large binary files and applicability paths from the file, in the form of check boxes in the package creation wizard. To perform a complete export, deselect the **Do not include package files** check box during Step 4 of the SPS Package Creation Wizard.

In order for the Secunia CSI to integrate with other patch deployment solutions, you need to create a configuration file, a script file and an applicability check script file:

- **Configuration file.** The configuration file is actually a representative of the tool and a visual integration between the Secunia CSI and that tool. The file is an xml file that should contain the tool name, script name and the input/setting fields required to configure the settings for the tool (text fields, radio buttons and check boxes are supported). When the Secunia CSI is launched it checks for the presence of any configuration file and, if there is a valid configuration file in the Extensions folder in the CSI path, it dynamically loads a GUI under the **Patching** menu of CSI. The configuration file also acts as an input file for the script.
- **Script file.** This script file corresponds to the SDK that the user has created to create and dispatch the package in the respective tool. The script file can be an executable, Java, VB, Python, or Perl script. Click **Publish** to execute the script file.
- **Applicability Check script file.** This script file runs the sps.exe on the computer if the applicability checks are cleared. This file is published together with the package to establish if the package is applicable to the system or not.

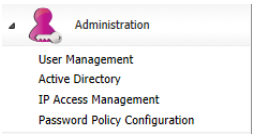
⚠ Running the script is a very strong feature. Use caution and ensure the sanity of the script file before publishing.

## Create and Publish the Package

1. Place the configuration and script files in the Extensions folder. The Extensions folder should be created in the same folder as the csi.exe.
2. Launch the Secunia CSI. If the configuration file format is valid, a configuration option will be visible under the **Patching** menu (for example, **Altiris Configuration**).
3. Click the configuration option to open a page where input and settings can be provided and saved.
4. Go to the SPS creation wizard. Complete all the package wizard fields or import a package. In Step 4 of 4: Applicability Criteria – Rules, there will be radio buttons allowing you to select the tool that you want to publish the package with. There will be as many selection options as there are valid configuration files.
5. Clicking **Publish** for any tool other than WSUS will run the script placed in the Extensions folder and named in the xml file.
6. The Secunia CSI waits for script to finish and, depending upon the execution of the script being successful or not, displays a message.
7. After successful publishing, the package can be seen in the respective tool.

# Administration

## Overview




The Secunia CSI 7.0 uses role based account management. Each CSI user is created and assigned a set of roles and limitations as appropriate. These roles determine which parts of the Secunia CSI the user has access to and limits what the user can view and scan.

Every user of the Secunia CSI can receive notifications such as reports, email and SMS.

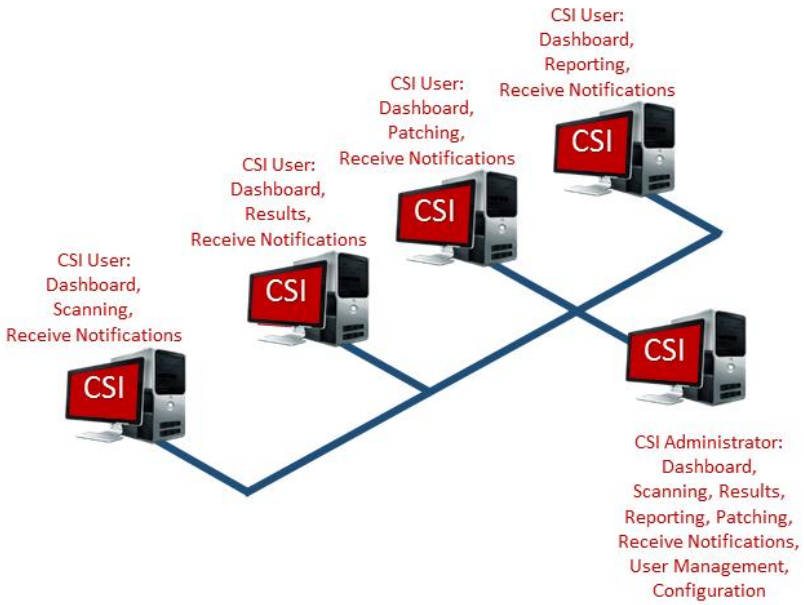
The roles are as follows:

- **Scanning –** Allows the user to scan hosts and view the **Scanning** menu of the Secunia CSI
  - Filter Scan Results **–** Allows the user to access and configure Whitelist and Blacklist filtering and Custom Scan Results
- **Results –** Allows the user to view scan results via, for example, Smart Groups
- **Reporting –** Allows the user to access various reporting options and the **Database Console** and **Database Cleanup** menus
  - Database Access **–** Allows the user to access the Database Console and schedule exports. There are no options to restrict the user's network access if this option is selected.
- **Patching –** Allows the user to access the Patching module
- VIM Integration **–** Allows the user to view and manage VIM accounts that have been verified and integrated with the Secunia CSI
- **Read Only –** Prohibits the user from making any changes that write data to the Secunia Cloud. Read Only users do not have Scanning or Patching capabilities.

Only the Root Administrator can access the Active Directory and Password Policy Configuration. Administrative users have additional capabilities that allow:

- Configuring the Secunia CSI
- Creating users and assigning their roles and restrictions
- Assigning License limits

None of the access limitations apply to an administrative user and they can view all Hosts and Results.


CSI User: Dashboard, Scanning, Receive Notifications
CSI
CSI User: Dashboard, Results, Receive Notifications
CSI
CSI User: Dashboard, Patching, Receive Notifications
CSI
CSI User: Dashboard, Reporting, Receive Notifications
CSI
CSI
CSI Administrator: Dashboard, Scanning, Results, Reporting, Patching, Receive Notifications, User Management, Configuration

# User Management

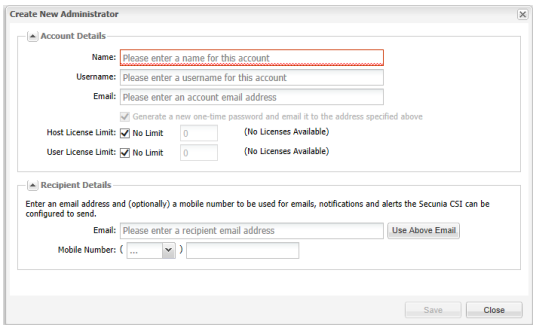
Use this page to administer your Secunia CSI users.

## Create a New Administrator

To create a new administration user account, click **Create New Administrator** and fill in the form, providing all the necessary details about the administrative user and include the limits to assign to the user.

An email will be sent to the user containing a welcome message and their Secunia CSI login credentials.

Right-click an existing account to view, edit or delete the account.

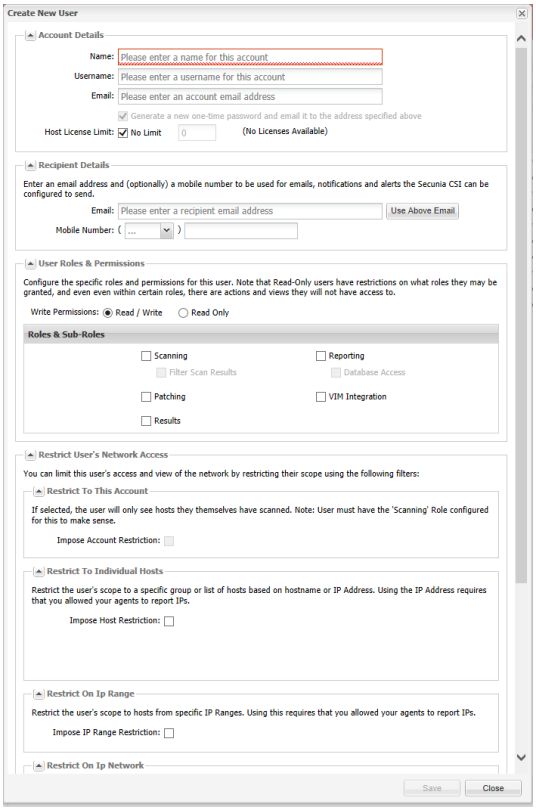

Create New Administrator
Account Details
Name:
Please enter a name for this account
Username:
Please enter a username for this account
Email:
Please enter an account email address
Generate a new one-time password and email it to the address specified above
Host License Limit:
No Limit
(No Licenses Available)
User License Limit:
No Limit
(No Licenses Available)
Recipient Details
Enter an email address and (optionally) a mobile number to be used for emails, notifications and alerts the Secunia CSI can be configured to send.
Email:
Please enter a recipient email address
Use Above Email
Mobile Number:
Save
Close

## Create a New User

To create a new user account, click **Create New User** and fill in the form, providing all the necessary details about the user. Select the **User Roles & Permissions** check boxes to assign the roles to the user.

A confirmation email with activation instructions will be sent to the email address provided.

Select the check boxes under **Restrict User's Network Access** to specify which network endpoints you would like to allow the user to have access to. You can use existing configured Hostname or IP Based Restrictions. Please refer to IP Access Management for further information.


Create New User
Account Details
Name:
Please enter a name for this account
Username:
Please enter a username for this account
Email:
Please enter an account email address
Generate a new one-time password and email it to the address specified above
Host License Limit:
No Limit
(No Licenses Available)
Recipient Details
Enter an email address and (optionally) a mobile number to be used for emails, notifications and alerts the Secunia CSI can be configured to send.
Email:
Please enter a recipient email address
Use Above Email
Mobile Number:
User Roles & Permissions
Configure the specific roles and permissions for this user. Note that Read-Only users have restrictions on what roles they may be granted, and even even within certain roles, there are actions and views they will not have access to.
Write Permissions:
Read / Write
Read Only
Roles & Sub-Roles
Scanning
Filter Scan Results
Reporting
Database Access
Patching
VIM Integration
Results
Restrict User's Network Access
You can limit this user's access and view of the network by restricting their scope using the following filters:
Restrict To This Account
If selected, the user will only see hosts they themselves have scanned. Note: User must have the 'Scanning' Role configured for this to make sense.
Impose Account Restriction:
Restrict To Individual Hosts
Restrict the user's scope to a specific group or list of hosts based on hostname or IP Address. Using the IP Address requires that you allowed your agents to report IPs.
Impose Host Restriction:
Restrict On Ip Range
Restrict the user's scope to hosts from specific IP Ranges. Using this requires that you allowed your agents to report IPs.
Impose IP Range Restriction:
Restrict On Ip Network
Save
Close

# Active Directory (Requires the Secunia CSI Plugin)

As a Root Administrator, you can select **Enable Active Directory integration** to allow your group policies to be automatically updated in the Secunia CSI when changes are made to the Active Directory.

> ⚠ Switching to Active Directory will hide your current Sites structure and the **Results > Sites** menu. For these to be displayed you must disable the Active Directory integration, logout, and then login to the Secunia CSI. It is **NOT** recommended to toggle Active Directory on and off unnecessarily.

Requirements to integrate the Secunia CSI with the Active Directory Domain:

- Active Directory Domain environment
- Domain Admin privileged account
- Port 3268 (msft-gc protocol) open between Domain Controller and CSI Host

Enabling Active Directory imports all discovered computer objects in the Active Directory Schema. Disabling Active Directory does not delete the computer objects in the Secunia CSI. Deleting sensitive computer information in the Secunia CSI must be done manually by the user.

Use the options below to control which Active Directory paths will be scanned. The Active Directory scanner will attempt to fetch the widest structure possible starting from the provided root location. The scanner only analyses Domain Controllers and Organizational Units.

- **All accessible branches** - By looking at the Active Directory Partitions, the scanner determines the accessible Domain Controllers that can be scanned.
- **Specific Domain Controller** - You can specify a certain Domain Controller to be scanned. It must be accessible from the host running the CSI.

The view options help you control how the elements of the Active Directory are displayed.

You can use the schedule options to set Active Directory scans at regular intervals.

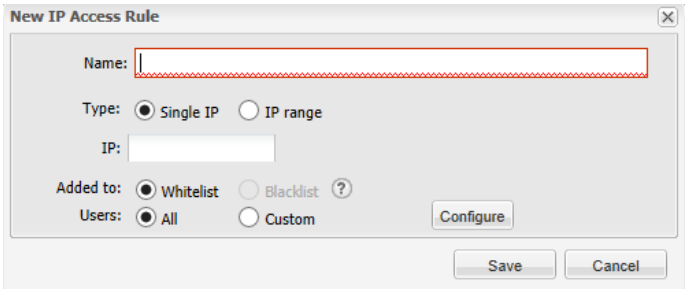
# IP Access Management (Requires the Secunia CSI Plugin)

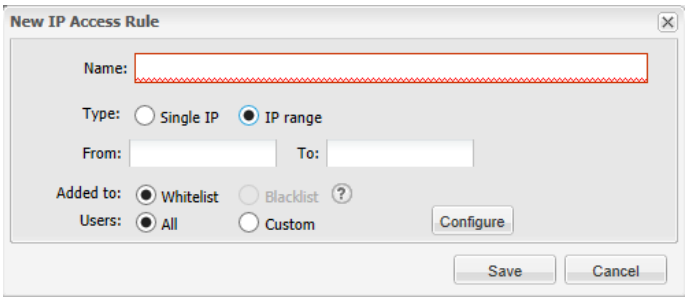
As a Root Administrator, you can use this page to configure the IP addresses the Secunia CSI console can be accessed from. Please note that you require administrative privileges to use this feature.

> ⚠ The first IP Access Rule you set up must always be a whitelist rule and must include the external (public) IP address of the console you are creating the rule from. If, for example, you check ipconfig you will find the internal IP address, which will not work. You can find your external IP address by using an Internet search engine and typing "find my ip address".

To create a new rule, click **New IP Rule**. Enter a name for the rule, the IP address or IP range, select to add the rule to a whitelist or blacklist, and the users to apply the rule to. The rule can contain a Single IP or an IP range, but you need to start with a whitelist rule. If you whitelist one IP address (the one you are using), then all other IP addresses are black-listed by default.

Once you have created a whitelist rule with an IP range, you can then blacklist a Single IP or an IP range within the whitelist IP range.



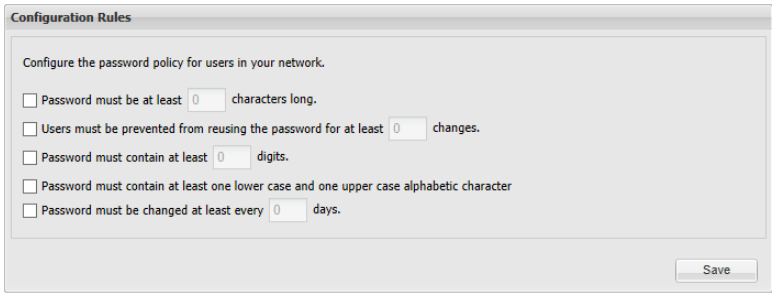




All IPs that have been added to a whitelist are able to use the Secunia CSI and IPs added to a blacklist are not able to connect.

To test if an IP has access to the Secunia CSI based on the current rules, click **Check IP**.

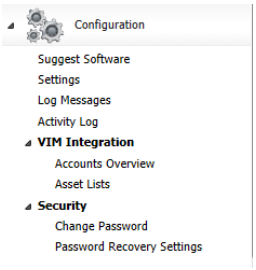
# Password Policy Configuration

Use this page to configure the password policy for users. This policy should be set on a "global" level, that is, the password policy cannot be configured differently for different users. The Administrator defines the policy based on the options displayed in the Configuration Rules dialog:


Configuration Rules
Configure the password policy for users in your network.
Password must be at least 0 characters long.
Users must be prevented from reusing the password for at least 0 changes.
Password must contain at least 0 digits.
Password must contain at least one lower case and one upper case alphabetic character
Password must be changed at least every 0 days.
Save

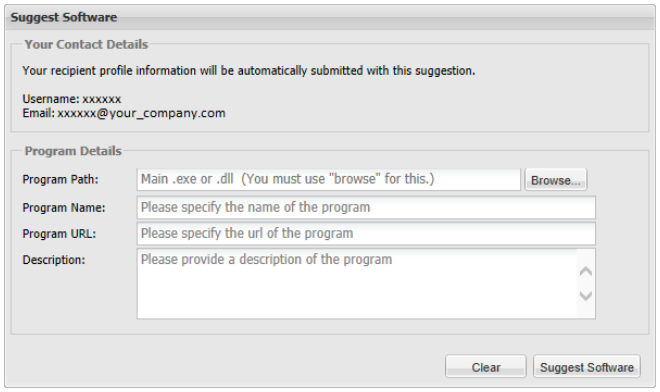
# Configuration

## Suggest Software




Use this page to send details about software that you would like to be added to the Secunia File Signature database.

It is important to enter as much information as possible to facilitate the processing and acceptance of your request.




## Settings

Use this page to configure various settings within the Secunia CSI.

### Scan Settings

Define the number of simultaneous scans to be executed. You can set the **Scan threads** value from 1 to 99 (the default is 5).

Please note that the number of simultaneous scan threads will not affect the scans being performed by the CSIA (Agent), since these scans are made locally by the agents.

### Instant Access

Select the **Activate Instant Access** check box to update your scan results as new Vulnerability Intelligence pertaining to your existing scan results emerges. By doing this you agree that you understand and accept that this is not a replacement for regular scheduled scanning, and could lead to your shown scan results not being the most accurate representation of the current state of your network.

### Collect Network Info

Select the **Activate Collect Network Info** check box to collect network hardware information, such as assigned IP address, when scanning devices. This option is only available to the Root Administrator.

### Zombie File Settings

Zombie files are files that were left behind after removing or applying a product/patch. The Secunia CSI will pick up these files since these are listed in the Secunia CSI file signature as being related to an Insecure or End-Of-Life product. Select **Hide Zombie Files** to ensure that zombie files do not appear in any of the scan results.

### Default Recipient Settings

Specify the default email and SMS recipient lists used throughout the CSI User Interface in various ways, including generating reports and configuring Smart Group notifications.

## Windows Update Settings

This setting controls the behavior of the Windows Update Agent (WUA) used by the Secunia CSI and CSI Agents to retrieve update information on Windows and other Microsoft products. You can select:

- Use a managed Windows Update server
- Use the official Windows Update server, providing updates to Windows only
- Use the official Microsoft Update server, providing updates to all Microsoft products including Windows, Word, Excel, and so on
- Use offline method: path to .CAB file

You should implement the .cab file scanning of windows update for clients that are not connected to Internet and cannot access WSUS or MU/WU. In such situations Microsoft provides a .cab file that can be used to scan the system. There are imitations to this feature:

1) You are responsible for getting the latest .cab file and placing it in a common share place accessible to all client computers.

2) The alternate scan data source (.cab file) only includes high priority updates (security bulletins, critical updates, update rollups) and some service packs. It does not include optional updates (updates, feature packs, tools) and some service packs. If a machine uses this source for scanning, then it is likely that fewer patches will be detected.

3) The CSI should be run as administrator.

⚠ Be aware that changing the **Windows Update Settings** may affect your scan results. For example, setting the WUA to use a WSUS to gather information about which OS updates are missing may result in missing important updates information if the WSUS is not fully synchronized with the official Windows Update server.

## Debug Logging

Select the **Enable Logging** check box to enable the Secunia CSI logging feature, which is useful when troubleshooting any issue that you may experience. In the event of a support request you can send the log file together any other relevant information to CSC@secunia.com. The log details can be seen in the log file and also within the Secunia CSI **Configuration > Log Messages > Log Details** page.

⚠ The **Enable Logging** feature requires additional resources to run and may decrease the performance of your CSI console if it is left to run continuously. Secunia recommends that this feature is enabled only when you have the need for extracting the relevant information.

# Log Messages

Use this page to view sequential data regarding the actions being performed by the Secunia CSI. It can also be used to detect and fix any issues that you might experience with the Secunia CSI console. The Log Details page becomes populated when you select the **Configuration > Settings > Debug Logging > Enable Logging** check box.

Right-click or double-click a message to copy the row data to the clipboard. Click **Clear** to remove all log entries. In the event of a support request you may be requested to provide relevant information from this page to CSC@secunia.com.

# Activity Log

Use this page to view information about user activity within the Secunia CSI, for example "write" actions, logins, and so on, with the exception of scans (due to the volume of data generated). You can access a full activity and login log for compliance monitoring and auditing purposes. Click the calendar icon next to the **From** and **To** fields to set a specific Activity Log date range to view. You can also use the **Search** field to filter the Activity Log results to specific actions, for example changes to IP access rules. You can also select **Show Priorities** to filter the results by High, Medium or Low Priority.

# VIM Integration

## Accounts Overview

Use this page to view and manage the VIM accounts that have been verified and integrated with the Secunia CSI.

To add a new account, click **Add Link** and enter your VIM Username and Password. Click **Verify and Integrate VIM Account**.

The VIM accounts, with the following columns, are displayed in the Account Overview page:

- VIM Account
- CSI Account
- Integration Date
- Asset Lists

Right-click an Account in the grid to remove it.

## Asset Lists

Use this page to view the Asset Lists created for the integrated VIM account. The Asset Lists are updated automatically with the Secunia CSI scan results.

Click **Create Asset List**. Enter the Asset List Name, select the VIM account from the drop-down list, select a Product Smart Group and click **Submit**.

When you create an asset list in the Secunia CSI, you can immediately see the new list in the Secunia VIM. The **Number of products**, **Number of vendors** and **End-Of-Life warnings** columns in the asset list in the Secunia VIM will be "0" until the products are synchronized. The **Synchronized Date** column displays when the asset list has been synchronized. If it has not yet been synchronized it simply displays a "-".

Only the **Number of products** and **End-Of-Life warnings** columns are synchronized to the VIM. The **Number of vendors** column is not populated and will always be "0". This is due to the fact that in VIM you can create asset lists based on either vendors (which would include all products from that vendor) or products (which is equivalent to getting a scan result from the Secunia CSI).

Right-click one or more asset lists and select **Edit Asset List** or **Delete Asset List** (login to the Secunia VIM to verify that the CSI asset lists have been deleted).

# Security

## Change Password

Use this page to change the Secunia CSI account password for the user that is currently logged in. The new password must contain a minimum of eight characters, or comply with the criteria defined in the Password Policy Configuration rules.

## Password Recovery Settings

Use this page to verify your email address and mobile number that will be used for password recovery. If your password is lost you can reset it at login using your verified email address and mobile number.

In the Contact Details fields you must provide your email address and a mobile phone number and click **Send Verification Codes**. The verification code will be received in two separate messages – one SMS on your mobile phone and the second via an email message. When entering your mobile phone number, you should select your country code from the drop-down list.

# Further Information

For answers to Frequently Asked Questions about the Secunia CSI patch management software, from scanning and patching advice to security compliance information and technical support, please visit:

http://secunia.com/vulnerability_scanning/corporate/faq/

To download product information regarding Vulnerability Scanning, Vulnerability Intelligence, Product Reviews, Product Installation and Technical User Guides, please visit:

http://secunia.com/vulnerability_scanning/corporate/resources/

# About Secunia

Secunia is a leading provider of IT security solutions that help businesses and private individuals globally manage and control vulnerability threats and risks across their networks and endpoints. This is enabled by Secunia's award-winning Vulnerability Intelligence, Vulnerability Assessment, and Patch Management solutions that ensure optimal and cost-effective protection of critical information assets.

Secunia's proven, complementary portfolio; renowned for its reliability, usability, and comprehensiveness, aids businesses in their handling of complex IT security risks and compliance requirements across industries and sectors – a key component in corporate risk management assessment, strategy, and implementation.

As a global player within IT security and Vulnerability Management, Secunia is recognized for its market-driven product development; having revolutionized the industry with verified and actionable Vulnerability Intelligence, simplified Patch Management, and automatic updating of third-party products.

Secunia plays an important role in the IT security ecosystem, and is the preferred supplier for enterprises and government agencies worldwide, counting Fortune 500 and Global 2000 businesses among its customer base. Secunia has operations in North America, the UK, and the Middle East, and is headquartered in Copenhagen, Denmark.

For more information, visit secunia.com

Follow Secunia

- Twitter: http://twitter.com/Secunia
- Facebook: http://www.facebook.com/Secunia
- Blog: http://secunia.com/blog/
- LinkedIn: http://www.linkedin.com/company/secunia

# Disclaimer

The contents of the Secunia website and all materials, information, links, documents and quotes ("Material") are provided "as is". Secunia does not, unless expressively provided otherwise in an agreement between you and Secunia or except as required by mandatory applicable law, either express or implied for the accuracy, warrant the accuracy, reliability or the contents of the Material.

Secunia and any of its licensor or partners are to the extent permitted by applicable law, under no circumstances responsible for any loss of data or income or any special, incidental, consequential or indirect damages howsoever caused.

Secunia assumes no responsibility for errors or omissions in the Material or software or other documents which are referenced by or linked to the Secunia website.

In no event shall Secunia be liable for any special, incidental, indirect or consequential damages of any kind, or any damages whatsoever. This includes without limitation, those resulting from (i) reliance on the material presented, (ii) cost of replacement goods (iii) loss of use, data or profits, (iv) delays or business interruptions, (v) and any theory of liability, arising out of or in connection with the use or performance of information. This applies irrespectively whether Secunia has been advised of the possibilities of such damages.

Secunia reserves the right to change any part of the Material without any notice.

For further information please visit
our website: secunia.com

Secunia
Mikado House
Rued Langgaards Vej 8
DK-2300 Copenhagen S
Denmark

Email: info@secunia.com
Phone: +45 7020 5144
Fax: +45 7020 5145

**Copyright 2013 Secunia. All rights reserved.**

This document may only be redistributed unedited and unaltered.
This document may be cited and referenced only if clearly crediting Secunia and this document as the source. Any other reproduction and redistribution in print or electronically is strictly prohibited without explicit permission.